IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Dealer Management Systems
Antitrust Litigation, MDL 2817

This document relates to:
Authenticom, Inc. v.
CDK Global, LLC, et al.,

No. 1:18-cv-868 (N.D. Ill.)

No. 1:18-CV-864

Hon. Robert M. Dow, Jr.

Magistrate Judge Jeffrey T. Gilbert

COUNTERPLAINTIFF THE REYNOLDS AND REYNOLDS COMPANY'S OPPOSITION TO COUNTERDEFENDANT AUTHENTICOM, INC.'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

RECORD CITATION FORMAT

Abbr.	Reference	Docket Number
Auth. Ex.	Exhibits to the Declaration of Daniel V. Dorris (*Authenticom*), May 20, 2020	Dkt. 977-1
Auth. SOF	Plaintiff Authenticom, Inc.'s Statement of Undisputed Material Facts in Support of Its Motion for Summary Judgment on Defendants' Counterclaims	Dkt. 977
CDK SJ Opp.	CDK Global, LLC's Opposition to Authenticom, Inc.'s Motion for Summary Judgment	Filed concurrently
Defs. Add'l Ex.	Exhibits to the Declaration of Daniel T. Fenske, July 28, 2020	Filed concurrently
Defs. JSUF	Defendants CDK Global, LLC and The Reynolds & Reynolds Company's Joint Statement of Common Undisputed Material Facts in Support of their Motion for Summary Judgment Exhibits, May 20, 2020	Dkt. 974
Defs. JSUF Ex.	Exhibits to the Declaration of Daniel T. Fenske, May 20, 2020	Dkt. 975
Mot.	Plaintiff Authenticom, Inc.'s Memorandum of Law in Support of its Motion for Summary Judgment on Defendants' Counterclaims	Dkt. 978
Resp. Auth. SOF	Response of Defendants CDK Global, LLC and The Reynolds and Reynolds Company to Plaintiff Authenticom, Inc.'s Statement of Undisputed Facts in Support of its Motion for Summary Judgment on Defendants' Counterclaims, July 28, 2020	Filed concurrently
RSUF	The Reynolds and Reynolds Company's Statement of Undisputed Material Facts in Support of Its Motion to Partial Summary Judgment, October 15, 2019	Dkt. 779 *et seq.*
RSUF Ex.	Exhibits to the Declaration of Brice Wilkinson, October 15, 2019	Dkt. 779-1

INTRODUCTION

For many years, Counter-Defendant Authenticom has engaged in a persistent campaign to access The Reynolds & Reynolds Company's proprietary DMS without a license, using illicit circumvention methods ranging from [redacted] These tactics, which are largely undisputed by Authenticom, establish liability against Authenticom as a matter of law on at least Reynolds's counterclaims under the Digital Millennium Copyright Act (DMCA) and the Wisconsin Computer Crime Statute. *See*, *e.g.*, Dkt. 785. In addition, these facts are more than sufficient to take Authenticom to trial on Reynolds's additional counterclaims for copyright infringement; violations of the Computer Fraud and Abuse Act (CFAA), California Comprehensive Computer Data Access and Fraud Act, and California Unfair Competition Law (UCL); and common law fraud, trespass to chattel, and unjust enrichment.

Now, in a stunning about-face from its prior pleadings and briefing throughout this litigation—which have uniformly emphasized that Reynolds's Dealer Management Systems (DMSs) license agreements prohibit dealers from allowing third-parties like Authenticom to access the Reynolds DMS—Authenticom argues for the first time in its Motion for Summary Judgment that Reynolds's license agreements actually *permitted* such hostile access after all.

Authenticom's prior pleadings to the contrary are unequivocal. In its 2017 Complaint, for example, Authenticom states that "[i]n their DMS contracts with dealers, both CDK and Reynolds require dealers to agree that they will not provide anyone other than the DMS provider access to their data for purposes of data integration and syndication to vendors," adding that "[t]he contractual terms thus prohibit dealers from granting access to their data to anyone else, including data integrators such as Authenticom." Defs. JSUF Ex. 90 (Authenticom Complaint [No. 17-cv-318 (W.D. Wis.) Dkt. 1]) ¶ 150.

As detailed in Section I.A below, Authenticom reiterated—and affirmatively relied on—Reynolds's contractual prohibitions again and again, including in its motion for preliminary injunction, Defs. Add'l Ex. 539 (Authenticom Mot. for PI [No. 17-cv-318 (W.D. Wis.) Dkt. 61]) at 1, 13; its statement of facts in support of that motion, Defs. JSUF Ex. 99 (Authenticom PI Statement of Facts [No. 17-cv-318 (W.D. Wis.) Dkt. 63]) ¶¶ 149, 153; its reply to Defendants' statement of facts in opposition to the motion for preliminary injunction, Defs. JSUF Ex. 94 (Authenticom PI Reply to Defs. Statement of Facts [No. 17-cv-318 (W.D. Wis.) Dkt. 146] ¶ 148; and its opposition to Defendants' motions to dismiss, Defs. Add'l Ex. 540 (Authenticom Cons. Opp. To Defs. Mot. to Dismiss [No. 17-cv-318 (W.D. Wis.) Dkt. 216]) at 15.

Authenticom consistently took that position (at least until now), because there is no way to seriously contend otherwise. The contracts themselves are unambiguous. Every court that has examined Reynolds's license agreements, including the Seventh Circuit and Judge St. Eve in this very litigation, has expressly agreed that Reynolds's DMS license agreements prohibit dealers from allowing third-party integrators to access the DMS. *See, e.g.*, *Authenticom, Inc. v. CDK Glob., LLC*, 874 F.3d 1019, 1022 (7th Cir. 2017) ("Reynolds . . . has always forbidden [data harvesting by third-party integrators] in its system licenses. . . . [T]he Reynolds licenses did not stop Authenticom from persuading some Reynolds users to permit it to scrape data from them as well, in violation of their agreements with Reynolds."). And Reynolds's system access policies have been publicized in the industry since at least 2006.

Authenticom's eleventh-hour attempt to rewrite the Reynolds DMS license agreements in an effort to fend off Reynolds's counterclaims, while perhaps understandable, is too late and in any event demonstrably wrong.

Authenticom's remaining arguments aimed at particular counterclaims also fail.

First, as explained in Reynolds's October 15, 2019 Motion for Partial Summary Judgment, it is beyond question that Authenticom has repeatedly "circumvent[ed] a technological measure that effectively controls access to a work protected under this title." That conclusively establishes liability under the DMCA. *See* Dkt. 785. Authenticom's argument that it is entitled to summary judgment that it is *not* liable under the DMCA relies primarily on tortured and incorrect interpretations of the terms "circumvention" and "effectively control access." In addition to being unsupported by any legal authorities, Authenticom's arguments are refuted by its own documents, in which Authenticom boasted about, by way of example only, [redacted] and its "workaround solutions that **circumvented Reynolds's efforts to block access**." Dkt. 785 at 6.

Authenticom's "copyrightability" and "fair use" arguments also fail as a matter of law—and come nowhere close to establishing the right to summary judgment *against* Reynolds's DMCA claims. Reynolds's protected works include the ERAccess and ERA-IGNITE PC application code, ERAccess and ERA-IGNITE screen displays, Reynolds DMS server-side software code, and the unique data compilation formats of data reports from the Reynolds DMS. These are classic copyrighted works, much of which has been registered with the U.S. Copyright Office. And even putting aside that most courts hold that "fair use" is not a defense to Section 1201 circumvention, Authenticom's nontransformative, commercial, wholesale copying is not fair use.

Second, Authenticom raises a statute of limitations argument, but this is solely an attempt to limit damages. Authenticom does not contend that any of Reynolds's claims are wholly time barred. And even as to Authenticom's attempt to limit damages, Authenticom badly misconstrues the relation-back doctrine and procedural history of this case.

Third, with respect to Reynolds's CFAA claim, without Authenticom's baseless argument that it was somehow "authorized" to access Reynolds's DMS, its motion rests entirely on the misguided argument that Reynolds cannot prove losses exceeding the CFAA's $5000 threshold. But even if Authenticom were correct (and it is not) that "aggregation" is not allowed, Reynolds's provable losses easily exceed $5000: Reynolds has spent approximately [redacted] per year to investigate and respond to unauthorized third-party access.

Fourth, Authenticom challenges Reynolds's claim for damages under the California UCL but completely ignores Reynolds's request for an injunction, i.e. "the primary form of relief available under the UCL."

Fifth, Authenticom's argument that Reynolds lacks an injury to establish its common law trespass to chattels claim fails because the weight of authority holds that large-scale unauthorized access alone is sufficient to establish this claim. Moreover, Reynolds also has substantial evidence of additional harm resulting from Authenticom's unauthorized access, including Authenticom's own expert's admission [redacted].

Sixth, Authenticom completely misses the mark with its assertion that Reynolds's claim for unjust enrichment is precluded by contract. Authenticom relies on inapposite authority regarding contracts *between the plaintiff and the defendant*, which has no relevance here.

Lastly, Reynolds can easily establish the challenged "misrepresentation" element for its fraud claim against Authenticom, particularly under Wisconsin's rule that "any conduct capable of being turned into a statement of fact is a representation." Based on the plain words on Reynolds's log-in screens and CAPTCHA prompts, Authenticom indisputably represented itself as a human, licensed user of the DMS. It was neither.

At the end of the day, we inevitably return to where we started: it is undisputed that Authenticom has engaged in a persistent campaign to access Reynolds's proprietary DMS without a license, using illicit circumvention methods ranging from [redacted] Authenticom's motion would have the Court hold that Reynolds has no remedy for that wrongful conduct, which cannot be—and is not—the law. Authenticom's motion for summary judgment should be denied.

ARGUMENT AND AUTHORITIES

I. Reynolds's DMS License Agreement Prohibits Authenticom's Access

Reynolds's DMS license agreements grant dealerships limited rights: only dealership employees [redacted].[1] Third-party data extractors are not dealership employees and therefore have no right under the license to access the Reynolds DMS at all, much less by [redacted] Every court to examine Reynolds's license agreements—including the trial court and the Seventh Circuit in this very case—has held that they prohibit access by parties like Authenticom. *See* Dkt.

[1] *See* Auth. Ex. 19, REYMDL00677044 [redacted] (emphasis added)).

176 at 15-16; *Authenticom*, 874 F.3d at 1022; *Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, 1:12-CV-848, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013) (in Reynolds DMS license, dealers "agree to prohibitions on connecting third-party applications to ERA" and "agree to prohibitions on allowing third-party integrators that are not licensed by Reynolds, like SIS, to interface with ERA."). And Authenticom itself pleaded, stipulated, and argued that the agreements prohibit dealers from providing Authenticom with access to the Reynolds DMS. Now, in a brazen about-face, Authenticom relies on two decontextualized sentences in the nearly 70-page license to claim that its access to the Reynolds DMS was ***permitted*** all along. Even if Authenticom could escape its prior representations to the Court so easily, its new position crumbles under scrutiny.

A. Authenticom Pleaded, Stipulated, and Argued That Reynolds's License Agreements Prohibited Authenticom's Access

The Reynolds DMS license agreement's prohibition on dealers permitting Authenticom to access the Reynolds DMS is a centerpiece of Authenticom's Complaint. *See* Defs. JSUF Ex. 90 (Authenticom Complaint [No. 17-cv-318 (W.D. Wis.) Dkt. 1]) ¶¶ 11, 150, 152-153, 156, 255. Moreover, Authenticom has repeatedly stipulated that the license prohibited Authenticom's access. Some examples:

- [redacted] Defs. JSUF Ex. 99 (Authenticom PI Statement of Facts [No. 17-cv-318 (W.D. Wis.) Dkt. 63]) ¶ 153.
- "In their DMS contracts with dealers, both CDK and Reynolds require dealers to agree that they will not provide anyone other than the DMS provider access to their data." *Id.* ¶ 149.
- "Defendants have implemented that agreement by prohibiting dealers from dealing with Authenticom (or other third-party integrators)." Defs. Add'l Ex. 539 (Authenticom Mot. for PI [No. 17-cv-318 (W.D. Wis.) Dkt. 61]) at 1. "Defendants' DMS contracts foreclose dealers from using other integration providers, including Authenticom. Reynolds prohibits dealers from [redacted] while

granting Reynolds the sole right [redacted] the dealer's data." *Id.* at 13 (citing Authenticom P.I. SOF ¶¶ 149, 153, 155).

- "It is undisputed that CDK and Reynolds' DMS contracts forbid dealers from allowing Authenticom or other parties from accessing the dealers' own data stored in the DMS." Defs. JSUF Ex. 94 (Authenticom PI Reply to Defs. Statement of Facts [No. 17-cv-318 (W.D. Wis.) Dkt. 146]) ¶ 148.

- "Reynolds prohibits dealers from 'provid[ing] access to [the DMS database] . . . to any third party' . . . ." Defs. Add'l Ex. 540 (Authenticom Cons. Opp. to Defs.' Mot. to Dismiss [No. 17-cv-318 (W.D. Wis.) Dkt. 216]) at 15.

- "CDK and Reynolds have exclusive dealing provisions in their dealer contracts (dealers cannot provide automated access to their data to anyone else) . . . . Reynolds prohibits dealers from 'provid[ing] access to [the DMS database] . . . to any third party' . . . ." Authenticom Cons. Br. for Appellee, No. 17-2540 (7th Cir.), Dkt. 52/58, at 21-22.

Whether Reynolds's DMS license prohibits Authenticom's access is not a live issue in this litigation: Authenticom's deliberate, clear, and unequivocal pleadings, stipulations, and arguments to this Court and the Seventh Circuit are binding and conclusive,[2] and Authenticom's Motion does not attempt to explain its drastic pivot. Authenticom's inevitable attempt to do so in its Reply brief should be rejected under standard waiver principles,[3] and in any event that attempt will be meritless: this Court has already correctly rejected Authenticom's attempts to backpedal its allegations that CDK's contracts prohibited Authenticom's access. *See* Dkt. 506 at 12 ("Authenticom[] argues that its allegation that CDK engaged in exclusive dealing by requiring dealers that use the CDK DMS exclusively for data integration services is legal argument and not a proper factual pleading. However, CDK is not citing to Authenticom's characterization of CDK's

[2] *E.g.*, *Keller v. United States*, 58 F.3d 1194, 1198 n.8 (7th Cir. 1995); *ecoNugenics, Inc. v. Bioenergy Life Sci., Inc.*, 355 F. Supp. 3d 785, 796 (D. Minn. 2019); *Monumental Life Ins. Co. v. Illinois Mut. Life Ins. Co.*, 2012 WL 5845631, at *2 (N.D. Ill. Nov. 19, 2012) (pleading that individual retired was binding despite argument as to meaning of "retirement" in contract); *Coe v. Milwaukee Cnty.*, 2008 WL 5071717, at *4 (E.D. Wis. 2008) (same where party attempted to change allegations about the existence of contract); *In re Brock Equip. Co.*, 2002 WL 88919, at *3 (N.D. Ill. Jan. 22, 2002) (pleading that defendant was party to contract was binding); *Weyerhaeuser Co. v. Israel Disc. Bank of New York*, 895 F. Supp. 636, 650 n.13 (S.D.N.Y. 1995) (undisputed fact in JPTO was binding as to interpretation of assignment letter).

[3] *E.g.*, *Darif v. Holder*, 739 F.3d 329, 336 (7th Cir. 2014) (arguments first raised in reply are waived).

actions as exclusive dealing. Rather, CDK is citing to the fact that Authenticom alleges that CDK's contracts prohibit dealers from granting Authenticom access to their data, ***which is a factual allegation***." (emphasis added)); *see also id*. n.3 ("the Court expects that Authenticom would not have alleged that CDK's contracts prohibit dealers from granting Authenticom access to their data unless it had a good faith basis for doing so").[4]

B. The License Unambiguously Prohibits Authenticom's Access

Authenticom was right: the Reynolds DMS license agreement unambiguously prohibits dealerships from permitting Authenticom to access the Reynolds DMS. And that is true regardless of whether the license permits access by "agents" (it does not) or whether Authenticom is an "agent" (it is not): Authenticom's ***methods*** of access are themselves prohibited. Authenticom's new argument to the contrary—focusing on CDK's, *not Reynolds's*, contracts—is meritless even absent Authenticom's binding admissions to the contrary.

The Reynolds DMS license agreement consists of [redacted] integrated documents: [redacted] The license is executed by signature [redacted] *E.g.*, Defs. JSUF Ex. 252, REYMDL00676893. The [redacted] *Id.* The [redacted] [redacted] *See* Auth. Ex. 19, REYMDL00677044 [redacted] Auth. Ex. 137, REYMDL00012246 [redacted] The [redacted] set out the terms and conditions applicable to every dealer's license agreement.

[4] Consistent with its position throughout this litigation, Authenticom did not plead a license defense based on the Reynolds dealer agreements in its answer, Dkt. 517 at 63-65, and so waived reliance on that agreement to defend against the copyright claim. Mot. 40 (written license is an affirmative defense); Fed. R. Civ. P. 8(c); *Castro v. Chicago Hous. Auth.*, 360 F.3d 721, 735 (7th Cir. 2004); *MCI Telecommunications Corp. v. Ameri-Tel, Inc.*, 852 F. Supp. 659, 666 (N.D. Ill. 1994).

And [redacted]. *E.g.*, Auth. Ex. 143, REYMDL00116206 at 219-223 [redacted] The [redacted] Auth Ex. 19, REYMDL00677044 [redacted]

Authenticom hangs its late-breaking "authorization" defense on two out-of-context sentences: the [redacted] and the [redacted] Mot. 24-28. Ignoring the rest of the contract, Authenticom spins from these provisions an unfettered license for the dealer's "agents" to use the DMS however they please. Nonsense.

Authenticom ignores myriad specific terms in the [redacted] that make clear that the general language Authenticom relies on does ***not*** grant permission for "agents" of the dealer to remotely access the Reynolds DMS. The license's terms expressly state that (1) [redacted]; and (2) [redacted] Authenticom's use of the Reynolds DMS fails both conditions, and so Authenticom's attempt to reinterpret the license is meritless.

1. The License Grants Access Rights Only to Dealership Employees

The [redacted] provide repeatedly that only dealership employees can access the DMS software:

- [redacted] Auth. Ex. 19, REYMDL00677044 [redacted] (emphasis added);
- [redacted] Auth. Ex. 137, REYMDL00012246 [redacted] (emphasis added).

These highly specific restrictions[5] control over the generic language of the first sentence of Section 1, both as a matter of ordinary contract law—the specific prevails over the general, *Harvard Mfg. Co. v. Sec. Pac. Bus. Credit (Ohio), Inc.*, 1986 WL 11962, at *5 (Ohio Ct. App. Oct. 23, 1986); Restatement (Second) of Contracts § 203(c)—and under [redacted] Auth. Ex. 19, REYMDL00677044 [redacted]

Authenticom's assertion, Mot. 25, 28, that "agents" are not "third parties" prohibited from accessing the DMS is illogical. The structure of the Master Agreement's access-limitation provision makes clear that "third party" bears its ordinary meaning: anyone other than the signatories to the contract. *E.g.*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("third party" means "[s]omeone who is not a party to a lawsuit, agreement, or other transaction but who is usu[ally] somehow implicated in it; someone other than the principal parties."). That is why the prohibition

[5] While these provisions speak most directly to the issue at hand, the [redacted] is replete with similar unambiguous language prohibiting dealers from allowing others to use the DMS software. *E.g.*, Auth. Ex. 137, REYMDL00012247 at -256 [redacted]; at -267 [redacted].

on third-party access is [redacted] The definition of [redacted] does not change that ordinary meaning. [redacted] on which Authenticom relies. It would be unnecessary to [redacted][6] A prohibition on providing access to [redacted] necessarily encompasses a prohibition on providing access to [redacted] Further, the [redacted] provision does not turn on third-party status at all: it is a categorical prohibition on [redacted] Authenticom's proposed interpretation would render these provisions meaningless surplusage: if anyone within the meaning of [redacted] has the right to access the DMS, these rigorously circumscribed access limitations drop out of the contract entirely. Authenticom's argument violates these basic rules of construction.

For the reasons stated in CDK's brief, CDK SJ Opp. § I.D, the doctrine of "implied license" has no bearing here. Reynolds's license [redacted] *Estate of Hevia v. Portrio Corp.*, 602 F.3d 34, 41 (1st Cir. 2010), and so Authenticom's argument, Mot. 26, fails.

[6] Moreover, as that definition makes clear, the phrase [redacted] Auth. Ex. 21, REYMDL00675678 [redacted] (emphasis added.) Mechanically importing the definition of [redacted] into the phrase [redacted] would convert that provision limiting the scope of the license into a dramatic expansion of the license, allowing access by [redacted] [redacted] Such illogical constructions are precisely why [redacted]

2. The License Bars Authenticom's Access Methods

Independent of those access limitations, the license agreement prohibits the ***means*** by which Authenticom accesses the Reynolds DMS. First, [redacted] Auth. Ex. 19, REYMDL00677044 [redacted] [redacted] *E.g.*, Auth. Ex. 143, REYMDL00116206 at 219-223 [redacted] Authenticom's Reynolds polling relies on [redacted] RSUF 26-28; Defs. JSUF 72-76. Thus, even if the license authorizes access by "agents" (it doesn't) and Authenticom is an "agent" (it isn't), Authenticom cannot shelter under the license: its use of Reynolds's software exceeds the scope of the license both as to number and location.

Second, the license provides that [redacted] Auth. Ex. 137, REYMDL00012246 [redacted] at -265. [redacted] Auth. Ex. 21, REYMDL00675678 [redacted] at -679. It is undisputed that Authenticom's polling process [redacted]. RSUF 28. Citing no evidence as to Reynolds, Authenticom once again lumps Reynolds's contracts in with CDK's in a cursory argument that this provision is inapplicable because "agents" are not "third parties." Mot. 28. That argument fails for the reason above: Authenticom is a third party under the Reynolds license.

Third, the license provides that [redacted] Auth. Ex. 137, REYMDL00012246 [redacted] at -267. Authenticom routinely engaged in precisely such conduct as part of its years-long efforts to [redacted], without which Authenticom's automated access to the DMS would have been impossible. RSUF 38-48. That too puts Authenticom's access to and use of the Reynolds DMS far outside the scope of the license, even assuming authorization for "agents."

3. Authenticom's Authorization Argument Fails For Additional Reasons

Taken together, these access and use restrictions make clear that [redacted] do not authorize Authenticom's access. The sentence [redacted][7] Those [redacted] establish that only dealership employees may access the software, [redacted], as set out above.

[7] [redacted]

If that were not enough, Authenticom's argument fails for two additional reasons. First, there is a reason that Authenticom's brief never provides the definition of [redacted] Auth. Ex. 21, REYMDL00675678 [redacted] at -679 (emphasis added). Authenticom's [redacted], RSUF 26-28; Defs. JSUF 72-76, is not a permitted [redacted] Second, Authenticom's business of [redacted], Defs. JSOAF 29, is not access [redacted] Authenticom provides no contrary argument.

In sum, the unambiguous terms of the license are clear that Reynolds's dealer licensees are prohibited from giving "agents" access to the Reynolds DMS software at all, much less by [redacted]

C. Course of Dealing Evidence Conclusively Rebuts Authenticom's Theory

Course of dealing is not properly relevant here given the license's unambiguous prohibition on Authenticom's access. *E.g.*, *Sunoco, Inc. (R & M) v. Toledo Edison Co.*, 953 N.E.2d 285, 292, ¶ 37 (Ohio 2011); *see also* Auth. Ex. 19, REYMDL00677044 [redacted] But to the extent the Court considers such evidence, there is overwhelming record proof that Reynolds has touted and enforced its contractual prohibitions on hostile access for over a decade. RSUF 10-19, 49; Defs. JSUF 80-88. In 2012, Reynolds sued a hostile integrator, SIS, for, among other things, tortious interference with the third-party access prohibitions in the Reynolds dealer license agreement.

Defs. JSUF 94-96. Authenticom has long been aware that Reynolds's license agreements prohibited its access. RSUF 49-56.

Authenticom's passing argument to the contrary is largely a tack-on to its CDK discussion, claiming only that Reynolds [redacted] and gave dealers the "practical ability to use data integrators" because Reynolds did not technologically restrict dealers' ability to create user credentials. Mot. 29. But there is no legitimate fact dispute here: [redacted] Defs. JSUF 89-90. [redacted]. Defs. JSUF 93, 119-127. The true course of dealing is that Reynolds successfully prohibited third-party access to its DMS, JSUF 86, 97-101, [redacted]. Authenticom's suggestion that Reynolds ever gave dealers "unfettered ability" to use hostile integrators is false and unsupported.

Authenticom's assertion that "Dealers . . . testified that they understood . . . that DMS access by their agents was allowed under their contracts with CDK and Reynolds," Mot. 30, is also a clear misrepresentation. [redacted] Defs. Add'l Ex. 549 [redacted]

[redacted], Defs. Add'l Ex. 544 [redacted]; Defs. JSOAF 1.

Thus, even if the Court were to consider extrinsic evidence, it indisputably proves that everyone long understood that Reynolds's DMS license agreements prohibited third-party access.

D. Authenticom is not an "Agent" of the Dealerships

In addition to the above contractual prohibitions, Authenticom is not an agent. Whether Authenticom is an "agent" within the meaning of the Reynolds license is governed by Ohio law. *See* Dkt. 506 at 13 n.4; Auth. Ex. 19, REYMDL00677044 [redacted]

Under Ohio law: (1) "the agent must have the power to alter the legal relations between the principal and third parties"; (2) "the agent must be a fiduciary of the principal in matters within the scope of the agency"; and (3) "the principal must have the right to control the agent's conduct of matters entrusted to her." *Eyerman v. Mary Kay Cosmetics, Inc.*, 967 F.2d 213, 219 (6th Cir. 1992). Authenticom presents no evidence or argument on the first two elements, which alone is fatal. Indeed, as set out in CDK's brief, Authenticom ultimately answered to vendors, not dealers [redacted] CDK SJ Opp. § I.B. [redacted] *See* Auth. Ex. 104 at CDK-0012577 [redacted] *Id.* at -584 [redacted] [redacted].[8] Authenticom certainly did not ***act*** as a fiduciary bound by duties of loyalty and

[8] The disclaimed relationships are precisely those that traditionally give rise to fiduciary duties. *See DeBoer Structures (U.S.A.) Inc. v. Shaffer Tent And Awning Co.*, 233 F. Supp. 2d 934, 946 (S.D. Ohio 2002) (joint venture), *accord Intercity Air Freight v. Lewensohn*, 301 N.W.2d 461, at *3 (Wis. Ct. App. 1980); *Dunn v.*

disclosure; to the contrary it [redacted], RSUF Ex. 72 at 5; [redacted], Defs. JSOAF 83, [redacted], Defs. JSOAF 35-44; and [redacted], Defs. JSUF 58; Resp. Auth. SOF 113; Defs. JSOAF 32-34, 38-39.

As to the third element, dealers did not exercise control over the means and methods that Authenticom used to scrape data from the DMS. The Ohio factors on this element of agency law cut decisively against Authenticom's "agency" defense:

> whether the employer or individual controls the details of the work; whether the individual is performing in the course of the employer's business rather than in an ancillary capacity; whether the individual receives compensation from the employer, and the method of that compensation; whether the employer or individual controls the hours worked; whether the employer or individual supplies the tools and place of work; whether the individual offers his services to the public at large or to one employer at a time; the length of employment; whether the employer has the right to terminate the individual at will; and whether the employer and individual believe that they have created an employment relationship.

William H. Evans, Jr. v. Ohio Attorney Gen. et al., 2020-Ohio-3471, ¶ 11. As set out in CDK's brief, [redacted]. CDK SJ Opp. § I.B.1 & B.2.a; *see also* Defs. JSOAF 3-31.

In addition to those contractual terms, the record confirms that ***Authenticom*** controlled "the manner or means of doing the work" and was "responsible to" the dealerships "only for the result." *Bostic v. Connor*, 524 N.E.2d 881, 883 (Ohio 1988). Authenticom's purported evidence of "dealer control," Mot. 32, is disputed, *see* Resp. Auth. SOF 25-26, 32-37, 39-40, but more

Zimmerman, 631 N.E.2d 1040, 1042 (Ohio 1994) (partnership), *accord Muehlmeier v. Tuffey*, 583 N.W.2d 673, at *4 (Wis. Ct. App. 1998).

importantly that evidence ultimately purports to establish only that dealers expect delivery of specified data fields to specified vendors at specified times. That is evidence of results, not manner or means. There is no evidence that dealers had any right or ability to control the technological details of *how* Authenticom performed its services—*e.g.*, its [redacted]. *E.g.*, Defs. JSOAF 3-31. Instead, the evidence shows that Authenticom controlled [redacted], *id.* 21-22; [redacted], *id.* 24; and [redacted], *id.* 19. Moreover, Authenticom [redacted] *id.* 20,[9] and [redacted], *id.* 36. Authenticom also [redacted]. *Id.* 37. Authenticom [redacted] *Id.* 41-44. Authenticom [redacted]. *Id.* 32-34. Authenticom's [redacted] *Id.* 25. Once Authenticom [redacted]. *Id.* 26, 83. For their part, the Dealership Class hotly denies knowledge of Authenticom's activities, Dkt. 965 at 57-63, and having any right to control that process, *id.* at 70-72.

Other Ohio factors similarly point against agency. Authenticom's business was an ancillary back-end service to dealerships, not provision of labor in the dealership's main business of selling

[9] Indeed, Authenticom [redacted] Defs. JSOAF 28.

cars. Authenticom performed its polling services from its Wisconsin headquarters, Resp. Auth. SOF 20, using its own tools—[redacted]—to access the DMS, RSUF 26-28. And it offered services to the market at large, not to one vendor or dealer at a time. In brief, Authenticom is a paradigmatic arm's-length independent contractor; the suggestion that it is the dealers' fiduciary agent is meritless.

Although Ohio law controls, Wisconsin law gives the same result. Agents must be fiduciaries,[10] and the factors are similar to Ohio's;[11] the above analysis applies. For the reasons set out in CDK's brief, Authenticom's reliance on *Lang v. Lions Club of Cudahy Wisconsin, Inc.*, 939 N.W.2d 582 (Wis. 2020), is inapposite; Wisconsin rejects agency on these facts, *Westmas v. Creekside Tree Serv., Inc.*, 907 N.W.2d 68, 77 (Wis. 2018). *See* CDK SJ Opp. § I.B.2.c.

II. Authenticom Flagrantly and Routinely Violated the DMCA

Authenticom violated Section 1201(a)(1)(A) of the DMCA every time it accessed the Reynolds DMS, and Authenticom's business—selling that hostile access—violates Sections 1201(a)(2) and 1201(b)(1).[12]

A. Authenticom's "Authorization" Defense Fails Under the DMCA

To establish an authorization defense under the DMCA, a defendant must prove it had specific authorization from the copyright owner to circumvent the access-control measures at issue. Mere authorization to access the copyrighted works protected by the measures is inadequate. *See, e.g.*, *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848, 863 (9th Cir. 2017); *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 953 n.16 (9th Cir. 2010); *Universal City*

[10] *Westmas v. Creekside Tree Serv., Inc.*, 907 N.W.2d 68, 77 (Wis. 2018) (emphasizing requirement of fiduciary duty). *Lang* is not to the contrary: the parties simply did not litigate that element. *See Lang*, 939 N.W.2d at 591.

[11] *See Pamperin v. Trinity Mem'l Hosp.*, 423 N.W.2d 848, 852 (Wis. 1988) (listing factors).

[12] Reynolds incorporates its DMCA liability arguments in its Motion for Partial Summary Judgment, *see* Dkt. 785, as if set forth fully herein.

Studios, Inc. v. Corley, 273 F.3d 429, 444 & n.15 (2d Cir. 2001); *Synopsys, Inc. v. InnoGrit,Corp.*, 2019 WL 2617091, at *3 (N.D. Cal. June 26, 2019). Even putting aside that Authenticom was not authorized to access the Reynolds DMS, period (*see* Section I, above), Reynolds certainly did not authorize Authenticom to circumvent the DMS access-control measures, and Authenticom has no evidence to the contrary. DMCA liability attaches regardless of any general authorization to "access the DMS," so Authenticom's authorization defense fails as a matter of law.

Authenticom's suggestion that this court should ignore the Second and Ninth Circuit's (as well as other courts') holdings should be rejected. The *Chamberlain* case Authenticom prefers (*Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004)) badly misreads the statute (as discussed in more detail in Section II.F, below). As relevant here, the phrase "without the authority of the copyright owner" in § 1201(a)(3)(A) refers to circumvention without authority, not access without authority. For the reasons well stated by the Second and Ninth Circuits, this Court should reject Authenticom's authorization defense.

B. Reynolds's Security Measures "Effectively Control Access," Whether Assessed Collectively or Individually

Reynolds's technological measures are access control measures under the DMCA. Authenticom's contrary position ignores the statute. To qualify under the DMCA, a technological measure must "effectively control access" to a protected work by requiring "the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). Reynolds's three technological measures at issue—CAPTCHA controls, Suspicious User ID, and password controls—indisputably meet this test.

These security measures should be assessed collectively as a matter of law and fact. *MDY*, 629 F.3d at 943 (assessing measures collectively); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311, at *7 (W.D. Wash. Jan. 18, 2000) (same). Reynolds's DMS access controls work together to form a powerful defense-in-depth, multifactor authentication system. Auth. Ex. 149, Tenaglia Rep. at 12; Defs. Add'l Ex. 530, Tenaglia Reply Report at 21 (describing possible authentication factors).[13] Reynolds's DMS requires passing through all its security measures. Authenticom argues for an inappropriate piecemeal treatment, identifying purported flaws with each measure that disappear when they are viewed holistically. While this approach is wrong, Reynolds's measures still satisfy the DMCA when viewed individually.

1. CAPTCHA

Reynolds's CAPTCHA prompts are a "technological measure that effectively controls access" as a matter of law. The test is that the measure must require the application of information, or a process or treatment, to gain access to the work. 17 U.S.C. § 1201(a)(3)(B). Every single court to consider the issue, including this Court in this case, has concluded that a CAPTCHA prompt falls within this definition. *See* Dkt. 506 at 17-18.[14] And rightly so: CAPTCHA requires the user to apply a process (their natural language-reading abilities) and information (the obscured text) to access the material behind the CAPTCHA.

Reynolds's CAPTCHAs took the conventional form, requiring the user to decipher and enter obscured text presented in a graphical image. *E.g.*, Mot. 51. As an additional protection,

[13] The username/password requires a user to demonstrate a knowledge factor, *i.e.* something you know. Subsequent CAPTCHA prompts require the user to demonstrate two distinct inherent factors, *i.e.* something you are (a human, [redacted].) All the while, Suspicious User ID measures require the user to demonstrate multiple behavioral factors, *i.e.* something you do (exhibiting usage patterns that match to "human" rather "bot," [redacted], etc.).

[14] *See also Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1166-67 (C.D. Cal. 2018) (collecting cases); *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018); *Craigslist, Inc. v. Kerbel*, 2012 WL 3166798, at *9–10 (N.D. Cal. Aug. 2, 2012) (collecting cases); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1056 (N.D. Cal. 2010); *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1111–12 (C.D. Cal. 2007). Authenticom's reliance on *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017), and Professor Kerr's article cited therein, is inapt for the simple reason that neither source purports to say *anything at all* about the DMCA, and instead address whether a CAPTCHA, without more, is sufficient to deny or revoke authorization to use a computer system under the CFAA.

[redacted]. RSUF 18. Reynolds requires ERA DMS users to answer CAPTCHAs in two scenarios: 1) [redacted], and 2) [redacted] Defs. JSOAF 58. Although the DMCA does not require it, there is record proof that these measures were "effective" in the real world, [redacted]. RSUF Ex. 26; *see also* Auth. Ex. 5 ¶ 37 (admitting these measures "first started disabling" Authenticom's services and made it "more difficult" to automatically access the DMS); Defs. JSOAF 46 (Authenticom's COO calling Reynolds's CAPTCHA prompts a [redacted] for Authenticom to overcome).

Desperate to escape this Court's prior holding on CAPTCHAs, Authenticom argues for a contorted rule: that only measures that comprehensively confirm that a user's access to the copyrighted work is authorized are "effective." Mot. 49-53. Authenticom cites no cases adopting its view, nor is Reynolds aware of any. This position has zero basis in the DMCA's text, which requires only that the measure involve the application of "information, or a process or treatment." Courts interpreting Section 1201(a)(3)(B) hold that the phrase "with the authority of the copyright owner" modifies "require": the measure must be one put in place by the copyright owner. *E.g.*, *MDY*, 629 F.3d at 954. And courts interpreting the mirror phrase in Section 1201(a)(3)(A)—"without the authority of the copyright owner"—reject the notion that authorization to access the work (as opposed to authorization to circumvent the access control) is the relevant criterion. *VidAngel*, 869 F.3d at 863; *MDY*, 629 F.3d at 953 n.16; *Corley*, 273 F.3d at 444 & n.15. If

Congress had intended to require that a measure must definitively confirm the user's authorization to access the work, it would have written a very different statute.

Unsurprisingly, courts routinely find that measures well short of Authenticom's artificial standard are "effective." *See, e.g.*, *MDY*, 629 F.3d at 936, 954. Even password controls—which Authenticom holds up as an archetypally effective access control—cannot ensure that the user is ***in fact*** authorized, as Authenticom's own actions (and business model) based on improperly obtained user credentials well demonstrate. Indeed, Authenticom's argument necessarily assumes that foundational DMCA cases were wrongly decided, beginning with the early and influential DVD decryption cases. *See Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom. Corley*, 273 F.3d 429. There, the studios encrypted DVDs with the "CSS" protocol and licensed the decryption algorithms to DVD-player manufacturers. *Corley*, 273 F.3d at 437. That encryption control acted, like CAPTCHA, as a categorical negative control: any device that applied the decryption algorithms could play the DVD, and any device that did not, could not. But there was no separate "authorization" test to ensure that the decryption algorithm was applied by a properly licensed player. More importantly, the code was readily discernible: a fifteen-year-old bought a licensed DVD player; reverse-engineered the decryption algorithm; and then distributed a "DeCSS" program that would apply that decryption algorithm on unlicensed devices, allowing them to play encrypted DVDs. *Reimerdes*, 111 F. Supp. 2d at 311. Notwithstanding its abject failure as an "authentication" measure, the court still concluded that CSS was an effective DMCA access control. *Id.* at 317-18. Courts continue to follow that holding, even though the CSS decryption algorithm is now widely available and has ***no*** ability to confirm user authorization.[15] Authenticom's rule would require the opposite result.

Authenticom is also wrong that Reynolds's CAPTCHAs perform no authorization or authentication role. Authenticom's own COO testified that he understood the purpose of Reynolds's CAPTCHAs to be [redacted] [redacted]." Defs. Add'l Ex. 548 (Clements Tr.) at 48:13-49:10; Defs. JSOAF 46. Mr. Clements was right: Reynolds's CAPTCHAs are a categorical authorization test that requires display of two distinct inherent—"something you are"—factors: [redacted]. Users who truthfully satisfy those factors are highly likely to be authorized dealership employees, whereas users that do not are *per se* unauthorized bots.[16] Like any access control, the measure has the potential to be both under- and overinclusive—that is why Reynolds deployed it as part of a multi-layered system of access controls, not as the sole DMS gatekeeper. But as Authenticom concedes, Mot. 54, the statute "does not require that an access control measure be strong or circumvention-proof," but rather only "requires an access control measure to provide some degree of control over access to a copyrighted work." *MDY*, 629 F.3d at 954. Reynolds's CAPTCHAs meet that benchmark.

Authenticom's purported expert testimony, Mot. 50-51, is misplaced. Ms. Miracle's opinions are contrary to the statute, the caselaw, and the entire body of scientific and technical

[15] *E.g.*, *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 932 (N.D. Cal. 2009); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1089, 1094-95 (N.D. Cal. 2004); *cf. Apple, Inc. v. Psystar Corp.*, 673 F. Supp. 2d 931, 941–42 (N.D. Cal. 2009), *aff'd*, 658 F.3d 1150 (9th Cir. 2011) (encryption control effective even when "decryption key for circumvention is publicly available on the internet").

[16] Authenticom's claim that Reynolds displayed the CAPTCHA answer "to the world," Mot. 51, is misplaced for precisely that reason: Reynolds displayed CAPTCHAs as an additional authorization test only to entities that had already represented—in Authenticom's case falsely—that they were an authorized dealership employee by logging into the system with a valid login/password combination.

sources in the record. *See* Dkt. 886; Dkt. 1032. The standard is a legal one, not subject to expert manipulation. To the extent the Court credits expert testimony over the statute's plain meaning, the great weight of expert authority favors Reynolds anyway. *See* Dkt. 886 at 8-9; Defs. Add'l Ex. 530, Tenaglia Reply Rep. at 20-22; Resp. Auth. SUF 110. For example, the federal government's National Institute for Standards and Technology defines "access control" as "the process of permitting or restricting access to applications at a granular level such as per user, ***per group*** and per resources." Resp. Auth. SOF 110. That is CAPTCHA's function. And CAPTCHAs ***are*** access-control measures as that term is understood in the computer-security field. Defs. Add'l Ex. 530, Tenaglia Reply Rep. at 20-22; Defs. Add'l Ex. 527, Schneck Reply Rep. ¶¶ 65-72.

2. Suspicious User ID

Reynolds's Suspicious User ID suite of security measures monitors user access patterns and activity on the ERA DMS. The measures themselves consist of software that runs on the PC applications and ERA DMS server. Defs. JSOAF 57. The measures detect indicia of automated use, [redacted] *Id.*; RSUF 15-18. [redacted] Defs. JSOAF 57. [redacted] *Id.*; RSUF 17-18.

Courts have repeatedly held that measures similar to the Suspicious User ID measures satisfy the DMCA—namely internal program measures that monitor for unauthorized access methods and prevent *further* access when a user fails a scan.[17] The Suspicious User ID program requires [redacted] in order to access the DMS. When a user fails those measures, their account is disabled and they lose the ability to access the Reynolds DMS and the copyrighted works therein. That is all Section 1201(a)(3)(B) requires.

Authenticom's "toehold" construction, under which the DMCA would not provide protection for defense-in-depth measures that prevent further access after a determined attacker initially breached defenses, is contrary to law. *See, e.g.*, *MDY*, 629 F.3d at 943; *Nexon*, 2013 WL 12121539, at *2. Authenticom's effort to distinguish those cases is unsupported and incorrect. *See* Mot. 55. The test is whether the measure requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201(a)(3)(b). The test is not "gain[ing] ***initial*** access to the work," and is not limited to protection of a system's perimeter defenses. Nor does the statute state or imply that an attacker who successfully gains access on one occasion is immunized to circumvent all access controls in the future to maintain that access. Such a construction would gut the statute by denying protection against precisely the serial offenders Congress targeted with per-circumvention statutory damages, *see* 17 U.S.C. § 1203(c)(3), by denying liability for every subsequent attack after an initial success. Indeed, courts routinely uphold DMCA claims for technological measures like CAPTCHA prompts that kick in sometime after the user has accessed part of the program or site in question. *See, e.g.*, *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018)

[17] *MDY*, 629 F.3d at 943 ("However, in our view, an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized."); *id.* at 954 (in-game scanning measure was effective access control because it "require[d] a 'process' in order for the user to ***continue accessing*** the work."); *Nexon Am., Inc. v. Game Anarchy, LLC*, 2013 WL 12121539, at *2 (C.D. Cal. Apr. 3, 2013).

& *id.*, No. 17-cv-7232, Dkt. 1 ¶ 21 (upholding violation for CAPTCHA prompt that appeared midway through ticket-ordering process); *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007) (same). Authenticom's suggestion that its (undisputable) hostile access is somehow forgiven by the DMCA would overturn well-settled DMCA case law and the plain language of the statute itself.

3. Login/Password Controls

Authenticom concedes that login/password controls are an effective access control measure under the DMCA. Mot. 50.

C. The Security Measures Control Access to a Copyrighted Work

1. Authenticom Understates the Scope of the Protected Works at Issue

Reynolds's measures control access to four copyrighted aspects of Reynolds's DMS: the ERAccess and ERA-IGNITE PC software code; the ERAccess and ERA-IGNITE screen displays; the Reynolds DMS server-side software code; and the unique compilation formats of data reports from the Reynolds DMS.

The Reynolds ERA DMS is a distributed software platform comprised of multiple copyrighted programs.[redacted]. Defs. JSUF Ex. 107 ¶¶ 2-3. Reynolds licenses two PC applications: ERAccess and ERA-IGNITE. *Id.* [redacted]. *Id.* [redacted] Defs. JSOAF 63.

Reynolds has registered copyrights for the ERAccess and ERA-IGNITE PC programs. RSUF 5. The registration for the program extends protection to the code and screen displays. *Fid.*

Info. Services, Inc. v. Debtdomain GLMS Pte Ltd., 09 CIV. 7589 LAK KNF, 2012 WL 1681792, at *3 (S.D.N.Y. May 15, 2012).[18] Registration is prima facie evidence of validity and copyrightability of the PC code and screen displays. 17 U.S.C. § 410(c); *Wildlife Exp. Corp. v. Carol Wright Sales, Inc.*, 18 F.3d 502, 507 (7th Cir. 1994).[19] That creates a rebuttable presumption; Authenticom has the burden to disprove copyrightability.[20] In any event, the PC application code and screen displays were natively developed and are highly creative, exhibiting significant subjective aesthetic judgment unconstrained by technical requirements. Defs. JSUF Ex. 107 ¶¶ 4-8; Defs. JSOAF 63-65.

The server-side software that a user accesses through use of the PC software is similarly copyrighted. That the copyright is not registered is irrelevant: copyright inheres at the moment of creation. *Fourth Estate Pub. Benefit Corp. v. Wall-Street.com, LLC*, 139 S.Ct. 881 (2019); *JCW Investments, Inc. v. Novelty, Inc.*, 482 F.3d 910, 914 (7th Cir. 2007). "[A]lmost all novel software code constitutes a creative, original work of authorship that is automatically protected under the Copyright Act." *Synopsys, Inc. v. AzurEngine Techs., Inc.*, 2019 WL 3842996, at *2 (S.D. Cal. Aug. 15, 2019). The server-side code was natively developed and is highly creative, exhibiting

[18] *See also Napoli v. Sears, Roebuck & Co.*, 874 F. Supp. 206, 211 (N.D. Ill. 1995), *vacated after settlement*, 926 F. Supp. 780 (N.D. Ill. 1996) ("[I]t is now beyond dispute that a copyright in a computer program extends to its screen displays."); United States Copyright Office, Circular 61 – Copyright Registration of Computer Programs, at 4-5, *available at* https://www.copyright.gov/circs/circ61.pdf ("A registration for a computer program covers the copyrightable expression in the program code and any copyrightable screen displays[.]").

[19] That Reynolds's registrations are for a particular version of the software is irrelevant: [redacted] Defs. JSUF 73, and the registration is therefore effective as to the earlier and later versions, *Selley v. Authorhouse, LLC*, 14-755, 2016 WL 5106938, at *2 (W.D. Pa. Sept. 20, 2016); *Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc.*, 275 F. Supp. 2d 543, 556 (D.N.J. 2003); *Well-Made Toy Mfg. Corp. v. Goffa Intern. Corp.*, 210 F. Supp. 2d 147, 158 (E.D.N.Y. 2002).

[20] *Fonar Corp. v. Domenick*, 105 F.3d 99, 104 (2d Cir. 1997); *Whimsicality, Inc. v. Rubie's Costume Co., Inc.*, 891 F.2d 452, 455 (2d Cir. 1989); *JCW Investments, Inc. v. Novelty, Inc.*, 289 F. Supp. 2d 1023, 1031 (N.D. Ill. 2003), *aff'd*, 482 F.3d 910 (7th Cir. 2007); *Marobie-Fl., Inc. v. Nat'l Ass'n of Fire Equip. Distributors*, 96 C 2966, 2000 WL 1053957, at *3 (N.D. Ill. July 31, 2000); *Kast v. Chrysler Corp.*, 96 C 6657, 1997 WL 305307, at *2 (N.D. Ill. May 30, 1997).

nearly infinite subjective expressive judgments, Defs. JSUF Ex. 107 ¶¶ 4-8; copyright thus attaches, *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1360–61 (Fed. Cir. 2014).

The compilation format of the data reports generated by the DMS are likewise copyrighted. The specific selection and arrangement of data fields within those reports was the result of Reynolds's creative selection and arrangement. Defs. JSOAF 66. Other DMS providers' databases contain similar raw facts, but different DMS providers' data reports are formatted differently and do not utilize the same labels or titles, ordering and arrangement, or structure. *Authenticom* Dkt. 1 ¶ 56; Defs. JSUF 3; Defs. JSOAF 66. Thus, the compilation format of the Reynolds DMS data reports is subject to copyright protection. *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 643 (7th Cir. 2003).[21]

Reynolds's security measures control access to all four copyrighted aspects of the Reynolds DMS. [redacted] Defs. JSOAF 59-61; Resp. Auth. SOF 108; Auth. SUF Ex. 155 (Miracle Rep.) ¶ 77, 79. [redacted] Defs. JSOAF 57; Resp. Auth. SOF 108. [redacted],[22] [redacted]

[21] Reynolds's license agreements and policy permit authorized dealership employees to send exported data reports to third parties of their choice, *see* Defs. JSUF 5, 9; however, that license does not permit unauthorized third parties like Authenticom to access and use the DMS software to generate and export reports themselves.

[22] Authenticom causing Reynolds code to be copied from the hard drive to RAM is copyright "copying," *Stenograph L.L.C. v. Bossard Assocs., Inc.*, 144 F.3d 96, 100 (D.C. Cir. 1998); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518-19 (9th Cir. 1993), regardless of whether that occurs on Reynolds

[redacted].[23] Defs. JSOAF 61. [redacted]. Defs. JSOAF 58, 62, 64-65.

Authenticom's Motion ignores the vast majority of that protection, and raises arguments only as to two copyrighted elements of the Reynolds DMS, [redacted]. Mot. 46-49. [redacted] And in any event, Authenticom's arguments as to the code and screen displays fail.

2. Authenticom Cannot "Access" Reynolds's Software Code

[redacted]. Auth Ex. 155, Miracle Rebuttal Rep. ¶ 77 [redacted] ¶ 79 [redacted]"); Resp. Auth. SOF 108;

servers, dealership computers, or Authenticom computers, *Apple Computer, Inc. v. Formula Int'l, Inc.*, 725 F.2d 521, 523-25 (9th Cir. 1984).

[23] [redacted]

Defs. JSOAF 60. [redacted]. Defs. JSOAF 59. Authenticom presents no evidence or argument that it could access the server-side code without passing those controls, [redacted]. Defs. JSOAF 60-61.

Moreover, Authenticom cites no evidence (and there is none) that it could view the text of the ERAccess or ERA-IGNITE PC software code at all (much less through ordinary operation of the program), and has no evidence of any method of accessing copyrighted screen displays other than launching the program and passing through security gates. Defs. JSOAF 60; Resp. Auth. SUF 108. These facts alone render *Lexmark* and *MDY*, Mot. 46-47, inapposite. In *Lexmark Intern., Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 546 (6th Cir. 2004), the court's reasoning was based on testimony that "[a]nyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence . . . ." *Id.* at 546-47 (citing hearing testimony). In *MDY*, the court of appeals affirmed the district court's similar rulings based on summary-judgment evidence that "[t]he user may view the code on the hard drive and may freely copy it to another hard drive, a CD, a jump drive, or other media," *MDY Indus., LLC v. Blizzard Entm't, Inc.*, CV-06-2555-PHX-DGC, 2008 WL 2757357, at *12 (D. Ariz. July 14, 2008), and trial evidence that "an owner of the game client software may use independently purchased computer programs to call up the visual images or the recorded sounds within the game client software" without logging onto Blizzard's servers that ran bot scans, *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 616 F. Supp. 2d 958, 965 (D. Ariz. 2009).[24] Authenticom has no similar evidence.

3. Authenticom's Copyrightability Arguments Are No Defense

Authenticom also makes a narrow copyrightability challenge, relying on its expert's testimony that two specific ERA-IGNITE screen displays—a progress bar and dialogue box—are functional and commonplace. Mot. at 48-49 (citing Ex. 155, Miracle Reb. Rep. ¶¶ 110-12). The apparent point of this argument is to show that the ERA-IGNITE CAPTCHAs that appear [redacted] do not protect any copyrighted content. That argument fails for a litany of reasons (and in any event it cannot support summary judgment, because Authenticom raises no corresponding argument as to ERAccess).

First, [redacted] Defs. JSOAF 62. Authenticom does not challenge the copyrightability of those works, leaving Reynolds's evidence unrebutted. Defs. JSUF Ex. 107 ¶¶ 4-8; Defs. JSUF 3; Defs. JSOAF 66. This whole argument is thus irrelevant to DMCA liability.

Second, Miracle's testimony—the only evidence Authenticom presents on this issue—is inadmissible. *See* Dkt. 886 at 17-19; Dkt. 1032 at 8-10. In the Seventh Circuit, copyrightability is a pure issue of law for which expert testimony is prohibited; that is why Authenticom has no in-circuit cases for its meritless argument, Mot. 48, that such testimony is required. *See* Dkt. 886 at

[24] In addition to being distinguishable, those decisions were wrong to the extent they held that the ability to access the work through use of sophisticated reverse-engineering methods sufficed to render the control ineffective. The DMCA speaks to the "ordinary course" of operation, *see* Section 1201(a)(3)(B); "plain reading of this statutory language means that access-control is at the level of the ordinary consumer," *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 932 (N.D. Cal. 2009). Even if Authenticom had evidence of similar reverse-engineering to that in *Lexmark* or *MDY*—it emphatically does not—that would be irrelevant. Ordinary users' only method of access to the software is through launching it, logging in, solving CAPTCHA, and behaving like a human user. Defs. JSOAF 56-61.

17-19; Dkt. 1032 at 8-10. Authenticom relies on authority from the wrong side of a circuit split: the Sixth and Ninth Circuits treat copyrightability as a fact issue, *see* Dkt. 1032 at 8-10.[25] Because Authenticom has not submitted competent controverting evidence, the registration presumption of copyrightability (and Reynolds's extensive evidence of the creative design of the DMS) is conclusive as set out above.

Third, even if Authenticom had presented competent evidence, the copyrightability challenge is procedurally barred. Miracle's copyrightability opinions—that the visual elements at issue are functional and commonplace, Mot. 48-49—go to the doctrines of merger and *scenes a faire*. Those doctrines are affirmative defenses. *Oracle Am., Inc. v. Google Inc.*, 750 F.3d 1339, 1358 (Fed. Cir. 2014); *Tensor Group, Inc. v. Glob. Web Sys., Inc.*, 1998 WL 887081, at *2 (N.D. Ill. Dec. 11, 1998). But Authenticom did not plead those defenses in its Answer. *See* Dkt. 517 at 63-65. The first indication Authenticom gave that it intended to present defenses based on merger and *scenes a faire* was Miracle's *rebuttal* expert report, served months after the close of fact discovery and with no opportunity for response. These defenses are therefore waived. Fed. R. Civ. P. 8(c); *Castro*, 360 F.3d at 735; *MCI Telecommunications Corp.*, 852 F. Supp. at 666. That Authenticom purports to couch these defenses as part of an "analytic dissection" or "abstraction-filtration-comparison" argument, Mot. 47-48, does not alter its burden to plead and prove them, *see* 4 Nimmer § 13.03[F][3]. The "filtration" step ***is*** application of merger and *scenes a faire, e.g.*, *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 838 (10th Cir. 1993); *Computer Associates Intern., Inc. v. Altai, Inc.*, 982 F.2d 693, 707-710 (2d Cir. 1992), and a party's failure

[25] In any event, the wrong-side-of-the-split cases Authenticom cites come nowhere near supporting a categorical rule that expert copyrightability testimony is mandatory whenever there is a computer in the vicinity. The only disputed copyrightability issue in this case is the visual creativity of two screen graphics; Miracle's purported "expert" analysis has nothing to do with technological creativity.

to properly present arguments for that analysis waives them as with any other argument, *Softel, Inc. v. Dragon Med. & Sci. Communications, Inc.*, 118 F.3d 955, 965 n.9 (2d Cir. 1997).

Fourth, even assuming Authenticom had presented competent evidence on a preserved defense, Authenticom misapplies merger and *scenes a faire* due to its mistaken reliance on substantial-similarity cases. Those doctrines only limit the ***extent*** of copyright protection for elements of a work subject only to a limited range of expression or that are commonplace in the genre. Even assuming Miracle is correct that "progress bars" and "dialogue boxes" ***as a category*** are functional or commonplace, Reynolds's specific implementation of progress bars and dialogue boxes retains protection against "virtually identical copying," as the very cases Authenticom cites, Mot. 47-49, make clear. *Incredible Techs., Inc. v. Virtual Techs., Inc.*, 400 F.3d 1007, 1014 (7th Cir. 2005); *Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1444 (9th Cir. 1994) ("Accordingly, protectable substantial similarity cannot be based on the mere use of overlapping windows, although, of course, Apple's *particular expression* may be protected."); *Atari, Inc. v. N. Am. Philips Consumer Elecs. Corp.*, 672 F.2d 607, 616 (7th Cir. 1982). The doctrines might limit Reynolds's ability to charge the producer of a different piece of software with infringement for using a visually distinct progress bar or dialogue box to report on a process. That is how the doctrine was applied in the substantial-similarity cases Authenticom cites, none of which involved literal copying. But a finding of merger or *scenes a faire* does not establish that there is ***no*** copyright protection, and some protection is all Reynolds must demonstrate under the DMCA.

Fifth, Reynolds's natively developed expression of a progress bar and dialogue box demonstrates the requisite spark of creativity for copyright protection. Copyright does not deal with novelty; if independently created and possessed of minimal creativity, even literally identical works are separately copyrightable. *Feist Publications, Inc. v. Rural Tel. Serv. Co., Inc.*, 499 U.S.

340, 345 (1991). And the "creativity" required for copyrightability bears a specific, noncolloquial meaning: "even a slight amount will suffice," and the standard is met even where the originality is "crude, humble, or obvious." *Id.* (quoting 1 Nimmer § 1.08[C][1]). There are virtually infinite ways to visually represent a progress indicator or a dialogue box; Reynolds made subjective aesthetic judgments. Defs. JSOAF 65.[26] Authenticom's copyrightability challenge therefore fails.

D. Authenticom Circumvented Reynolds's Access-Control Measures

The record evidence overwhelmingly establishes Authenticom's dogged determination to establish and maintain access to the Reynolds DMS by—in its own [redacted]. RSUF Ex. 99, AUTH_00280842, at 845 (emphasis added).[27]

1. CAPTCHA

[redacted]

RSUF Ex. 36, AUTH_00167914; RSUF 45-47.

[26] Consider the progress indicator: there is an initial choice between several categories of indicator (bar, hourglass, clock, etc.). Even after settling on "progress bar," the creator must make a series of subjective aesthetic judgments as to the shape of the bar itself (oval or rectangular; rounded or squared edges; length and width of the bar); color scheme (what color the progress bar fills in as it advances toward completion, what shade of that color, whether the color intensity varies across the bar or is the same); ornamentation of the bar as it fills (does it remain solid, or is it separated into vertical blocks or diagonal slices or candy-stripes, or does color intensity vary to give a shimmering effect, etc.).

[27] Authenticom's lawyers described things just the same way until Reynolds filed these counterclaims: Authenticom confessed in this lawsuit that it had worked to "develop workaround solutions that circumvented Reynolds's efforts to block access." Mot. for P.I. at 8 [*Authenticom* Dkt. 61] (emphasis added); Authenticom Cons. Br. for Appellee, No. 17-2540 (7th Cir.), Dkt. 52/58, at 12 ("Reynolds' efforts, however, were not entirely successful; Authenticom, CDK, and other integrators worked with dealers to develop workarounds.").

Every single court to have considered the issue, including this Court in this case, has determined that using automated methods and CAPTCHA farms to respond to CAPTCHA prompts is circumvention under the DMCA.[28] And Authenticom's conduct goes far beyond that in the *Ticketmaster/Craigslist* line. First, beginning in August 2011, [redacted] *See* Resp. Auth. SOF 98 & Defs. Add'l Ex. 401, AUTH_00169080 at -80_0002-3; RSUF 31-32. [redacted] RSUF 32 & Ex. 49. Authenticom submitted no competent evidence that it ***ever*** stopped using that method, Resp. Auth. SOF 98,[29] and the plausible inference is that the practice continued forward. [redacted] is a heartland DMCA violation, and Authenticom provides no argument to the contrary.

Authenticom supplemented its [redacted] with Eastern European CAPTCHA farms, [redacted]

[28] *See* Dkt. 506 at 17-18; *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1166-67 (C.D. Cal. 2018) (collecting cases); *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018); *Craigslist, Inc. v. Kerbel*, C-11-3309 EMC, 2012 WL 3166798, at *9–10 (N.D. Cal. Aug. 2, 2012) (collecting cases); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1056 (N.D. Cal. 2010); *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1111–12 (C.D. Cal. 2007).

[29] The only evidence Authenticom cites—its COO Brian Clements's declaration claiming with extraordinary specificity that Authenticom used the process only briefly in 2013 and 2014 and "definitively ceased using" the program in June 2014, *see* Auth. SOF 98 & Ex. 165 at ¶¶ 10-11—is contradicted by Mr. Clements's deposition testimony that he did ***not*** know that timeframe. Defs. Add'l Ex. 548 (Clements Tr.) 131:13-19. That portion of his declaration is a classic "sham affidavit" that the Court should disregard. *James v. Hale*, 959 F.3d 307, 315-16 (7th Cir. 2020); *Bryant v. U.S. Steel Corp.*, 428 Fed. Appx. 895, 897 (11th Cir. 2011) (sham-affidavit exclusion where "Bryant's affidavit, in which she stated that she remembered the exact date on which she received the right-to-sue letter, flatly contradicted her earlier deposition testimony, in which she stated that she did not remember the date"). Mr. Clements's declaration is further contradicted by Authenticom's documents: Authenticom's CEO Steve Cottrell stated in August 2013 that [redacted] Defs. Add'l Ex. 401, AUTH_00169080 at -80_0002-3. The reason Reynolds does not have more granular evidence of Authenticom's use of these methods is that Authenticom has—despite its preservation obligations—continuously destroyed its polling logs throughout this litigation. *See* Dkt. 711 at 1-8.

[redacted] [redacted]. RSUF 33-34. [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]. RSUF 35-37. These too are straightforward DMCA violations. Dkt. 506 at 17 (citing *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018)). [redacted] easily qualifies as "bypassing" the CAPTCHA, as Authenticom's own expert admitted, Resp. Auth. SOF 91, and further as "impairing"[30] and "avoiding"[31] the CAPTCHA.

Second, unlike the defendants in the *Ticketmaster* and *Craigslist* line of cases, Authenticom also [redacted]. RSUF 45-47. Authenticom's own characterization is a stark confession of DMCA liability: [redacted] RSUF Ex. 36, AUTH_00167914. Such technological trickery is the hallmark of DMCA liability, and courts consistently hold that similar efforts to "spoof" a device's characteristics in order to [redacted] and therefore [redacted] a technological measure that requires confirmation of those characteristics is DMCA circumvention. *See Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018) ("Defendants' use of colocation facilities and other methods, such as deleting tracking tools like 'cookies,' are also actionable under the DMCA if used to circumvent Ticketmaster's technological measures."); *Synopsys, Inc. v. InnoGrit, Corp.*, 19-CV-02082-LHK, 2019 WL 2617091, at *3 (N.D. Cal. June 26, 2019) (holding that changing the MAC addresses on computers to run unauthorized software is DMCA

[30] *See* Merriam-Webster, https://www.merriam-webster.com/dictionary/impair ("impair" is "to diminish in function, ability, or quality: to weaken or make worse."); *see also Point 4 Data Corp. v. Tri-State Surgical Supply & Equip., Ltd.*, 2012 WL 3306600, at *12 (E.D.N.Y. June 13, 2012) ("By including terms such as 'avoid' and 'bypass,' Congress plainly intended section 1201(a)(1) to cover a wide array of acts.").

[31] *See* Merriam-Webster, https://www.merriam-webster.com/dictionary/avoid ("avoid" is "to prevent the occurrence ***or effectiveness of***" (emphasis added)).

circumvention); *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, at *4, 7 (W.D. Wash. Jan. 18, 2000) (circumvention where "the Streambox VCR is able to convince the RealServer into thinking that the VCR is, in fact, a RealPlayer").

The Court has already roundly rejected application of the *I.M.S.* line of password-misuse cases Authenticom cites,[32] including this Court's decision in *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *5 (N.D. Ill. Sept. 20, 2012), in the distinct context of CAPTCHA circumvention. *See* Dkt. 506 at 17-18. Authenticom's account of the Court's reasoning, Mot. 43-44, is through-the-looking-glass revisionism. That opinion did not ***mention*** CDK's allegation that Authenticom "cracked" CAPTCHA, much less rely on it. The Court followed the unanimous view: use of automated bots and CAPTCHA farms is circumvention because it "bypassed" and "avoided" the CAPTCHA control. *Id.* at 17.

Authenticom's argument that "complying with" an access control can never be circumvention, Mot. 41-43, is simply wrong: courts routinely find that application of real, but unauthorized, encryption algorithms and access keys is circumvention. In *Reimerdes*, the DeCSS program did nothing more than "comply with" the CSS access control by applying the real decryption algorithm—but the court easily found circumvention because "[o]ne cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license." 111 F. Supp. 2d at 317-18. Courts follow *Reimerdes*'s lead in finding circumvention on similar facts.[33] To the extent there is a tension between these cases and the

[32] *See I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004).

[33] *E.g.*, *Synopsys, Inc. v. InnoGrit, Corp.*, 19-CV-02082-LHK, 2019 WL 4848387, at *8–9 (N.D. Cal. Oct. 1, 2019) (use of real, but unauthorized, license key to activate software was circumvention); *Dish Network, L.L.C. v. Vicxon Corp.*, 12-CV-9-L WVG, 2013 WL 3894905, at *2-3, *6–7 (S.D. Cal. July 26, 2013) (use

Navistar/*I.M.S.* line, a contention this Court has already rejected, Dkt. 506 at 16-17, *I.M.S.* and its progeny are distinguishable. That line ultimately stands for the narrow proposition that using a misappropriated password "precisely as intended" is not circumvention, *Synopsys, Inc. v. InnoGrit, Corp.*, 2019 WL 4848387, at *9 (N.D. Cal. Oct. 1, 2019), but that is not this case. Reynolds precisely intended for its CAPTCHAs to be answered by [redacted] in the dealership. Authenticom's multilayered technological chicanery is far afield. *Id.*

Finally, even if Authenticom were correct that its [redacted] were not circumvention in themselves, that is no refuge: Authenticom provides no defense of its [redacted], which involve a distinct circumvention of [redacted]

2. Suspicious User ID

Authenticom does not dispute that it worked constantly to disguise its automated access to the Reynolds DMS as legitimate access by authorized dealership employees. Authenticom [redacted]. RSUF 39. Authenticom [redacted]

of unauthorized, but real, decryption algorithm was circumvention); *Apple, Inc. v. Psystar Corp.*, 673 F. Supp. 2d 931, 941–42 (N.D. Cal. 2009), aff'd, 658 F.3d 1150 (9th Cir. 2011) (use of real and publicly available, but unauthorized, decryption algorithm was circumvention); *Microsoft Corp. v. EEE Bus. Inc.*, 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008) (use of unauthorized, but real, license key was circumvention); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004) ("However, while 321's software does use the authorized [CSS] key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses CSS."); *Paramount Pictures Corp. v. 321 Studios*, 03-CV-8970 (RO), 2004 WL 402756, at *1-2 (S.D.N.Y. Mar. 3, 2004).

[redacted]. RSUF 40-43.[34] Authenticom [redacted] RSUF 44. And Authenticom [redacted]. RSUF 45-48.

Nor does Authenticom dispute that evading similar measures through similar means is circumvention under the DMCA.[35] From at least May 2013 forward, RSUF 17, every time Authenticom polled the Reynolds DMS and extracted data, it [redacted]. Had it not done so, [redacted]. Defs. JSOAF 57. As such, Authenticom's argument that Reynolds has not submitted evidence of circumvention but only "attempted" circumvention is puzzling: ***every instance*** of Authenticom's automated access to the Reynolds DMS [redacted] Defendants' damages expert, Professor Rubinfeld, sets out a painstaking, conservative accounting of such access. Auth. Ex. 152, Rubinfeld (Reynolds) Rep. ¶¶ 73-77.

3. Login/Password Controls

Each time Authenticom accessed the Reynolds DMS, it [redacted]. RSUF 23-25; *see* Section I, *supra*. Authenticom's effort to seek refuge under *Navistar* and *I.M.S.* is misguided: those cases were

[34] Indeed, Authenticom explicitly stated in internal communications that [redacted] RSUF Ex. 72 at 5 (emphasis added).

[35] *MDY*, 629 F.3d at 954; *Synopsys*, 2019 WL 2617091, at *3 (N.D. Cal. June 26, 2019) (changing computer MAC addresses); *Synopsys*, 2019 WL 4848387, at *9 ("manipulation of the InnoGrit computers' identifying information . . . constitutes circumvention"); *Ticketmaster*, 306 F. Supp. 3d at 1174 ("use of colocation facilities and . . . deleting tracking tools like 'cookies'"); *Nexon*, 2013 WL 12121539, at *2.

wrongly decided. The better-reasoned line of cases rejects *I.M.S.* and its progeny and imposes DMCA liability on these facts. *See, e.g.*, *Actuate Corp. v. Int'l Bus. Machines Corp.*, 2010 WL 1340519, at *9 (N.D. Cal. Apr. 5, 2010); *see also Synopsys, Inc. v. InnoGrit, Corp.*, 2019 WL 4848387, at *8 (N.D. Cal. Oct. 1, 2019) (collecting cases rejecting *I.M.S.* line).

Two interpretive errors undermine the *I.M.S.* line's reasoning. First, in imposing a requirement that circumvention occurs only when the defendant "hacks around" a measure, *e.g. I.M.S.*, 307 F. Supp. 2d at 532, the *I.M.S.* line ignores the statutory text. Under Section 1201(a)(3)(A), decryption and descrambling are both within the category of avoiding, bypassing, removing, deactivating, or impairing a technological measure: that is why the statute uses the phrase "or otherwise" to link those two terms to the laundry list that follows. Yet neither descrambling nor decrypting a work involves "hacking around" an access control; as discussed in detail above, courts routinely impose liability for use of a real, but unauthorized, decryption key. Use of a real, but unauthorized, password is no different, and thus should be treated similarly under the DMCA. *Actuate*, 2010 WL 1340519, at *9 ("[A] combination to a lock appears to be essentially the same as a password. Nor does the Court find support in the statute itself for drawing a distinction between passwords and other types of code that might be used for decryption.").

Second, and closely related, the *I.M.S.* decision hinged its holding on a flawed analogy to *Reimerdes* and *Corley* that turns the facts in those cases on their head:

> Defendant did not surmount or puncture or evade any technological measure to do so; instead, it used a password intentionally issued by plaintiff to another entity. As an analogy to *Universal Studios*, the password defendant used to enter plaintiff's webservice was the DVD player, not the DeCSS decryption code, or some alternate avenue of access not sponsored by the copyright owner (like a skeleton key, or neutralizing device). Plaintiff, however, did not authorize defendant to utilize the DVD player. Plaintiff authorized someone else to use the DVD player, and defendant borrowed it without plaintiff's permission.

Id. at 532-33. But contrary to that lynchpin reasoning, the DeCSS program was nothing other than "a password intentionally issued . . . to another entity," *id.*, that the aforementioned teenaged hacker obtained from a licensed DVD player. *Reimerdes*, 111 F. Supp. 2d at 311; *Corley* 273 F.3d at 437. The defendants in *Reimerdes* and *Corley* were found liable on exactly the facts *I.M.S.* held could not create liability: the studios "authorized someone else to use" the DVD decryption algorithm, and the defendants "borrowed" the algorithm without the studios' "permission." *I.M.S.*, 307 F. Supp. 2d 532-33; *contra Reimerdes*, 111 F. Supp. 2d at 311, 317-18 (finding circumvention where "[o]ne cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license"); *Corley*, 273 F.3d at 437. Even if *I.M.S.*'s reasoning were correct, it would be inapplicable in this case, where Authenticom emphatically did ***not*** use passwords "precisely as intended": its very business model was a large-scale hacking campaign that used technological trickery at every turn to obtain and maintain unauthorized and uncompensated access to and use of Reynolds's intellectual property for its own profit. *Synopsys*, 2019 WL 4848387, at *9. Authenticom's [redacted] is DMCA circumvention under the statutory text and the better-reasoned line of authority.

E. Reynolds's Section 1201(a)(2) and Section 1201(b)(1) Claims

Sections 1201(a)(2) and 1201(b)(1) of the DMCA prohibit Authenticom's trafficking in circumvention technology. *See* 17 U.S.C. §§ 1201(a)(2), 1201(b)(1) ("[n]o person shall . . . , offer to the public, provide, or otherwise traffic in any technology, . . . service, . . . or part thereof, that" "is primarily designed for," "has only limited commercially significant purpose . . . other than to," or "is marketed . . . for use in" circumvention of access or anticopying controls). Authenticom's footnote-only argument, Mot. 41 n.19, that Reynolds cannot recover on these claims is meritless. Authenticom's passing argument that Reynolds has not established circumvention under Section

1201(a)(1)(A) fails as set out above. And the survival of Reynolds's Section 1201(a)(1)(A) claim has no bearing on the Section 1201(b)(1) claim, for which copyright infringement (which survives because Authenticom was not licensed and its copying was not fair use) is the relevant "direct" offense, *MDY*, 629 F.3d at 945, not circumvention of access controls. Authenticom's suggestion that Reynolds lacks a damages model is mistaken: Professor Rubinfeld's report establishes the inputs. For 1201(a)(2) and 1201(b)(1) violations, the statute provides for damages of "not less than $200 or more than $2500 per . . . device, product, component, offer, or performance of service, as the court considers just." 17 U.S.C. § 1203(3)(A). Here, the relevant metric is "performance of service": Authenticom's trafficking violation was the sale of its polling service on a per-vendor, per-dealer, per-month basis. Defs. JSUF Ex. 74 (Lawton Rep.) ¶ 259, 275. Rubinfeld calculated Authenticom's total per-vendor, per-dealer, per-month automated, nonexempted polling services, *see* Auth. Ex. 152, Rubinfeld (Reynolds) Rep. ¶¶ 66 ([redacted] on legacy Authenticom), 70 [redacted] on DealerVault). That amounts to ([redacted]) * $200 = [redacted] in damages at the bottom end; ([redacted]) * $2500 = [redacted] in damages at the top end.

F. There Is No "Infringement Nexus" Element

Contrary to Authenticom's contention, there is no "infringement nexus" requirement for claims under Sections 1201(a)(1)(A) and 1201(a)(2) of the DMCA: those provisions "extend[] a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to works protected under Title 17, i.e., copyrighted works," regardless of whether the circumvention of an access control facilitates copyright infringement. *MDY*, 629 F.3d at 943-52. As the *MDY* court persuasively explained, *Chamberlain*—Authenticom's key authority—was wrongly decided.[36]

[36] While some district courts in the Seventh Circuit followed *Chamberlain* before *MDY* was decided, *see* Mot. 55-56, no court in this Circuit appears to have adopted *Chamberlain* since *MDY* was decided. The only post-*MDY* in-circuit decision Authenticom cites, *Couponcabin LLC v. Savings.com, Inc.*, 2016 WL

The vast weight of authority rejects fair use as a defense to Section 1201(a) claims.[37] In any event, *Chamberlain* is irrelevant here: its "infringement nexus" requirement does not apply where, as here, the copyright owner imposed contractual restrictions prohibiting third-party access. *See Chamberlain*, 381 F.3d at 1183, 1202 n.17. To the extent the Court determines that *Chamberlain* is not distinguishable, it should reject *Chamberlain* and its progeny as wrongly decided.

Section 1201(a)'s focus on measures that control access is distinct from traditional copyright, under which "access" to a work is not an exclusive right, *see* 17 U.S.C. § 106, and circumvention to access a work is not in and of itself infringement. *MDY*, 629 F.3d at 945. By contrast, Section 1201(b)(1) speaks directly to traditional copyright, prohibiting trafficking in circumvention technology for measures that that "protect[] ***a right of a copyright owner under this title*** in a work or a portion thereof." That linkage, absent from Section 1201(a), makes clear that the Section 1201(a) prohibitions extend "a new form of protection": a right to sue for circumvention, regardless of whether the access facilitates infringement. *MDY*, 629 F.3d at 944.[38]

Authenticom's preferred "infringement nexus" requirement renders meaningless the detailed administrative-law scheme in Section 1201(a)(1)(B)-(D). Those provisions give the Librarian and Registrar (not the courts) the power to establish fair-use-analogous exemptions to

3181826, at *5–6 (N.D. Ind. June 8, 2016), expressly acknowledged the circuit split, declined to resolve it, and dismissed on a different ground.

[37] *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 & n.13 (2d Cir. 2001) (affirming district court's conclusion in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 322–23 (S.D.N.Y. 2000) that fair use is not a defense to Section 1201(a)); *Dish Network L.L.C. v. Ramirez*, 2016 WL 3092184, at *3 (N.D. Cal. June 2, 2016); *DISH Network LLC v. New Era Elecs. Corp.*, 2013 WL 5486798, at *4 (C.D. Cal. Sept. 27, 2013); *Dish Network, L.L.C. v. Vicxon Corp.*, 2013 WL 3894905, at *6 (S.D. Cal. July 26, 2013); *In re Maxim Integrated Prods., Inc.*, 2013 WL 12141373, at *19 (W.D. Pa. Mar. 19, 2013); *DISH Network, L.L.C. v. Sonicview USA, Inc.*, 2012 WL 1965279, at *7 (S.D. Cal. May 31, 2012); *United States v. Crippen*, 2010 WL 7198205, at *2 (C.D. Cal. Nov. 23, 2010); *Macrovision v. Sima Prods. Corp.*, 2006 WL 1063284, at *2 (S.D.N.Y. Apr. 20, 2006). The Copyright Office has expressed the same view. *See MDY*, 629 F.3d at 948 n.10.

[38] Authenticom's suggestion that the *MDY* court "overlooked that § 1201(a)(2) and § 1201(b)(1) apply to different types of access controls," Mot. at 57, is puzzling, as that distinction was the basis for the Ninth Circuit's decision.

Section 1201(a)(1)(A)'s prohibition, but only for "noninfringing uses" of the underlying copyrighted work. That power would be "unnecessary if an infringement nexus requirement existed," *MDY*, 629 F.3d at 950, because circumvention to enable noninfringing access would never violate Section 1201(a) in the first place. Further, imposing an "infringement nexus" requirement on Section 1201(a) claims would render all of Section 1201(a) surplusage: every violation of Section 1201(a)(1)(A)-plus-infringement-nexus would already be unlawful as copyright infringement; every violation of Section 1201(a)(2)-plus-infringement-nexus would already be unlawful as a violation of Section 1201(b)(1). *MDY*, 629 F.3d at 946.[39]

Chamberlain suffers from other flaws as well. First, it mistakenly relies on Section 1201(c)(1) (which provides that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title") to import an infringement nexus into Section 1201(a) claims. 381 F.3d at 1193. That provision does not change the scope of Section 1201(a). It "simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred." *Corley*, 273 F.3d at 443.[40] Second, the *Chamberlain* court read the phrase "without the authority of the copyright owner" in Section 1201(a)(3)(A) to require that the defendant's access to the work was unauthorized. 381 F.3d at 1193. But that phrase expressly refers only to authorization to

[39] Moreover, while legislative history is irrelevant given the unambiguous statutory text, *e.g. N.L.R.B. v. SW Gen., Inc.*, 137 S. Ct. 929, 941-42 (2017), the legislative history confirms that Congress intended to create a distinct, standalone prohibition on circumvention of access controls that did not turn on whether the resulting access was infringement. *See MDY*, 629 F.3d at 946-47 (collecting committee reports); *Corley*, 273 F.3d at 443 & n.13 (explaining that legislative history did not permit interpretation under which fair use was defense to Section 1201(a) claims).

[40] *See also MDY*, 629 F.3d at 949-50 (holding that Section 1201(c)(1) does not affect scope of Section 1201(a); instead it emphasizes that Congress created a "new anti-circumvention right" that "does not limit the traditional framework of exclusive rights created by § 106, or defenses to those rights such as fair use.").

descramble, decrypt, or otherwise bypass a measure, not authorization to access the work. 17 U.S.C. § 1201(a)(3)(A); *MDY*, 629 F.3d at 953 n.16; *Corley*, 273 F.3d at 444 & n.14.

Third, the *Chamberlain* court mistakenly observed that "virtually every clause of § 1201 that mentions 'access' links 'access' to 'protection.'" 381 F.3d at 1197. But only Section 1201(b)(1) includes such a linkage. Section 1201(a) does not link "access" to the "***rights*** protected under the Copyright Act": it prohibits circumvention of measures that control access to ***works*** protected under the Copyright Act. The "works protected" phrase does not speak to the type of access (infringing or not). The remainder of the *Chamberlain* court's reasoning turned on policy objections, but Congress addressed those concerns in Section 1201(a)(1)(B)-(D), which the court missed. Those concerns also cannot trump the statute's unambiguous language. *See Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 188 (1994).

G. Authenticom's Fair Use Defense Fails

In any event, Authenticom's infringement defense fails on the merits. Authenticom does not dispute that it engages in routine [redacted] RSUF 26-28, instead relying solely on the affirmative defense of fair use.[41] Authenticom bears the burden to come forward with undisputed evidence satisfying the statutory factors under 17 U.S.C. § 107. *Chicago Bd. of Educ. v. Substance, Inc.*, 354 F.3d 624, 629 (7th Cir. 2003). Tellingly, its brief never mentions those factors.

Instead, Authenticom relies on *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640, 644–45 (7th Cir. 2003), to urge an "intermediate copying" fair-use defense. In that case, neither party suggested that the defendant's pursuit of public-domain tax-assessment records

[41] Other than its license argument, which fails for reasons discussed in Section I, fair use is the only basis on which Authenticom moves that applies to Reynolds's copyright infringement claim. Because Authenticom does not have a license and its conceded copying of Reynolds's software was not fair use, the Court should deny summary judgment on the copyright claim.

would require copying of the plaintiff's software; the case concerned only a data-compilation copyright on the format in which the assessment records were stored within a Microsoft Access database at each relevant municipality. The defendant did not plead or argue fair use, and specifically disclaimed any argument that it was entitled to copy the plaintiff's software or the actual formatting in the Microsoft Access databases.[42] The court's noninfringement ruling—based on undisputed evidence that the defendant could obtain that open-records data without copying the plaintiff's software or compilation formats, 350 F.3d at 644, resolved all issues presented in the record and briefing. The follow-on disquisition into the intermediate copying defense was classic dictum. *See United States v. Crawley*, 837 F.2d 291, 292–93 (7th Cir. 1988).

Even if that dictum sufficed to import the "intermediate copying" defense to the Seventh Circuit, Authenticom cannot (and has not attempted to) satisfy its requirements. The defense is narrow: the cases "do[] not stand for the proposition that ***any*** form of copyright infringement is privileged as long as it is done as part of an effort to" ascertain noncopyrightable information. *DSC Comm'c'ns Corp. v. Pulse Comm'c'ns, Inc.*, 170 F.3d 1354, 1363 (Fed. Cir. 1999) (emphasis added). Instead, the defense only applies when (1) the defendant legitimately obtained "an authorized copy" of the copyrighted work,[43] and (2) limited copying in the course of research and development efforts is the ***only*** way to ascertain noncopyrightable information embedded in the

[42] *See* Brief of Defendant-Appellant, *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 2003 WL 22721368 (C.A.7), at *13-14.

[43] *Atari Games Corp. v. Nintendo of Am. Inc.*, 975 F.2d 832, 843 (Fed. Cir. 1992); *see also Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 609 (9th Cir. 2000) ("Connectix's reverse engineering of the Sony BIOS extracted from a Sony PlayStation console ***purchased by Connectix engineers*** is protected as a fair use." (emphasis added)); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1514–15 (9th Cir. 1992), as amended (Jan. 6, 1993) ("Accolade purchased a Genesis console and three Sega game cartridges ….").

copyrighted work.[44] The defense is inapplicable when the copying is nothing more than "ordinary operation" of the copyrighted software, *DSC*, 170 F.3d at 1363, and where the infringer does nothing more than "commandeer[]" the copyrighted work to "us[e] it for the very purpose for which" legitimate licensees acquire it, *Triad Sys. Corp. v. Se. Exp. Co.*, 64 F.3d 1330, 1336–37 (9th Cir. 1995).[45]

Authenticom fails all of these criteria. [redacted] RSUF 27.[46] That alone defeats a finding of fair use. *Atari*, 975 F.2d at 843. Second, Authenticom's copying was not "necessary," *Sony*, 203 F.3d at 602, or the "only way," *Sega*, 977 F.2d at 1527, to ascertain noncopyrightable raw data stored in the Reynolds DMS. The Reynolds DMS's reporting functionality, including Dynamic Reporting, allows dealers to export their data and furnish it to Authenticom and other vendors, all consistent with their license agreements and Reynolds's policies. Defs. JSUF 5, 9. That Authenticom [redacted]"

[44] *WIREdata*, 350 F.3d at 644 ("AT would lose this copyright case even if the raw data were so entangled with Market Drive that they ***could not be extracted*** without making a copy of the program. . . . [I]f ***the only way*** WIREdata could obtain public-domain data . . . would be by copying the data . . . as embedded in Market Drive . . . because the data and the format in which they were organized ***could not be disentangled***, it would be privileged to make such a copy[.]" (emphasis added)); *Sony*, 203 F.3d at 603 ("Connectix's copying of the Sony BIOS ***must have been 'necessary'*** to have been fair use." (emphasis added)); *Sega*, 977 F.2d at 1527 (fair use when copying is the "***only way*** to gain access to the ideas and functional elements embodied in a copyrighted computer program" (emphasis added)); *Atari*, 975 F.2d at 843 ("The fair use reproductions of a computer program ***must not exceed what is necessary*** to understand the unprotected elements of the work. . . . Any reproduction of protectable expression must be ***strictly necessary*** to ascertain the bounds of protected information within the work." (emphasis added)).

[45] While certain aspects of *Triad*'s holding were "legislatively overruled" by 17 U.S.C. § 117(c)—which establishes an infringement defense for software copying incident to repairing and servicing machines—the Ninth Circuit regards its reasoning as valid and binding outside the specific Section 117(c) context. *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1158-59 (9th Cir. 2011). Authenticom has not, and could not, raise a Section 117(c) defense, and so *Triad*'s reasoning remains persuasive as sister-circuit authority.

[46] As explained above in Section I, Reynolds's dealer licenses expressly prohibited Authenticom's access to and copying of the Reynolds DMS software.

[redacted] Defs. JSUF 37-41, conclusively establishes that Authenticom's copying was not fair use under the "intermediate copying" doctrine. That is precisely why the District Court for the District of Arizona recently rejected a materially identical fair-use argument by Kellogg Hansen's client in related litigation.[47] Third, Authenticom used the Reynolds software to perform the same sort of tasks that the software was designed to perform. Auth. SOF 27.[48] That "commandeering" of Reynolds's software is far afield from the narrow fair-use protection for R&D reverse-engineering Authenticom relies on, *DSC*, 170 F.3d at 1363; *Triad*, 64 F.3d at 1336-37, particularly given that Authenticom's purpose was to develop a competing database to undercut Reynolds, *Snap-on Bus. Sols. Inc. v. O'Neil & Associates, Inc.*, 708 F. Supp. 2d 669, 686 (N.D. Ohio 2010) (distinguishing *WIREdata*).[49]

[47] *CDK Glob. LLC v. Brnovich*, 2020 WL 2559913, at *6 (D. Ariz. May 20, 2020) ("Here, Reynolds has alleged that, even if third parties do not have access to their DMS, 'dealership customers can use dealer-driven data export tools to send their operational and inventory data to application providers or other third parties, as the dealer deems appropriate.' Thus, unlike in *Sony* and *WIREdata*, third parties' copying of [CDK and Reynolds's] software would presumably not be necessary to obtain dealer data and thus would presumably not qualify as 'fair use.'") (citations omitted). The fact that dealers can export their data in a non-infringing manner (and one affirmatively permitted by Reynolds) also renders the *WIREdata* court's policy concerns inapplicable here: Reynolds is not "trying to secrete the data in its copyrighted program." 350 F.3d at 641-42.

[48] Of course, Authenticom's *automated* use of the software introduced significant security and system performance concerns—the DMS software that Authenticom copied was designed to be used by human employees, and is not built to process automated access. Defs. JSUF 43-48, 51; Resp. Auth. SOF 27. But that does not affect the distinction at issue between research-and-development copying and ordinary-use copying set out in *DSC* and *Triad*.

[49] In addition to *WIREdata*, Authenticom cites cursory analysis from several related district court opinions, but in all three both the parties and court misapplied the "intermediate copying" fair use defense by failing to recognize or discuss the "necessity" element that *WIREdata*, *Sony*, *Sega*, and *Atari* uniformly and unambiguously require. In *Phantomalert, Inc. v. Google Inc.*, 2016 WL 879758, at *11 (N.D. Cal. Mar. 8, 2016), the plaintiff "did not challenge Defendants' reliance on *Assessment Technologies* in their Motion and does not appear to dispute that copying merely to extract information for use in the Waze application would not give rise to a claim for copyright infringement," and the court failed to address the necessity element of the defense at all. So too in *NTE, LLC v. Kenny Constr. Co.*, 2016 WL 1623290, at *5 (N.D. Ill. Apr. 25, 2016): there is no discussion, or indeed mention, of the necessity element in the parties' briefing or the courts' decision. *See, e.g.*, Defendant's Memorandum in Support of its Summary Judgment Motion, Dkt. 86 at 8-12, 2015 WL 9791822, *NTE LLC v. Kenny Construction Co.*, No. 1:14-cv-09558 (N.D. Ill. Nov. 5, 2015) (failing to brief necessity element); Plaintiff's Response in Opposition to Defendant's Motion for Summary Judgment, Dkt. 94 at 13-14, 2015 WL 9791750, *NTE LLC v. Kenny Construction Co.*, No.

Authenticom therefore cannot prevail on the only fair-use argument it raised in its Motion. Moreover, though its failure to brief the statutory factors waives any reply-brief argument, Reynolds notes that *every* Section 107 factor weighs against fair use. *See* 17 U.S.C. § 107(1)-(4). The first factor looks to (1) whether the use was transformative and (2) whether the use was commercial. *Oracle Am., Inc. v. Google LLC,* 886 F.3d 1179, 1196 (Fed. Cir. 2018), *cert. granted*, 140 S. Ct. 520 (2019) [hereinafter *Oracle II*]. That Authenticom's purely commercial use is unlike Section 107's exemplar categories—"criticism, comment, news reporting, teaching . . . , scholarship, or research"—weighs heavily against transformative use. *Id.* at 1199-1200. And "creat[ing] exact copies of . . . software" and "put[ting] those copies to the identical purpose as the original software" is nontransformative as a matter of law.[50]

The second factor—nature of the work—similarly weighs against fair use. The programs at issue are products of significant investment, highly creative, and thus entitled to stronger protection than the compilations at issue in *WIREdata*, *Phantomalert*, and *Kenny*. *Advanced Computer Servs. of Mich., Inc. v. MAI Sys. Corp.*, 845 F. Supp. 356, 365 (E.D. Va. 1994).

The third factor—amount and substantiality of copying—weighs heavily against fair use, because Authenticom [redacted]

1:14-cv-09558 (N.D. Ill. Dec. 4, 2015) (same). The briefs in *Evolution, Inc. v. SunTrust Bank*, 342 F. Supp. 2d 943, 956 (D. Kan. 2004) similarly do not discuss the necessity element, *see* Defendants' Memorandum in Support of Motion for Summary Judgment, No. 2:01-cv-02409-CM, Dkt. 126 at 32-34 (D. Kan.); Plaintiff's Response in Opposition, No. 2:01-cv-02409-CM, Dkt. 142 at 55-57, and the court did not discuss it. These cases simply misstate the law.

[50] *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d 769, 778 (9th Cir. 2006); *see also Oracle II*, 886 F.3d at 1200; *Triad*, 64 F.3d at 1336-37; *cf. Worldwide Church of God v. Philadelphia Church of God, Inc.*, 227 F.3d 1110, 1117 (9th Cir. 2000) (wholesale copying for supplanting use "seriously weakens a claimed fair use").

The fourth factor—impact on the market and value of the work—points strongly against fair use. That analysis considers both the market for the work and derivative markets, *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 568 (1985), and requires the court to "consider not only the extent of market harm caused by the particular actions of the alleged infringer, but also whether unrestricted and widespread conduct of the sort engaged in by the defendant . . . would result in a substantially adverse impact on the potential market for the original." *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 590 (1994) (citation and quotation marks omitted). Verbatim copying for commercial purposes—like Authenticom's—is presumptively harmful, *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 451 (1984), and the movant bears the burden of introducing "favorable evidence" to rebut the presumption, *Campbell*, 510 U.S. at 590. Authenticom introduced no evidence to rebut the presumption, which is therefore conclusive. And the impact of behavior like Authenticom's, if unrestricted and widespread, would be devastating: Reynolds would be denied license fees for its copyrighted software and would continue to be undercut by Authenticom's free-riding. *Wall Data*, 447 F.3d at 781-82; *Triad*, 64 F.3d at 1337; *Advanced Computer Servs.*, 845 F. Supp. at 366; *cf. In re Indep. Serv. Organizations Antitrust Litig.*, 1997 WL 161941, at *3 (D. Kan. Mar. 12, 1997).

In sum, Authenticom's large-scale, profit-oriented, nontransformative [redacted] copying of Reynolds's software is far beyond the bounds of fair use. The defense fails as a matter of law.

III. Authenticom Is Not Entitled to Summary Judgment Based on Limitations

Authenticom offers several limitations arguments in its Motion, but none is a valid basis for summary judgment. Reynolds's claims are not time-barred, and Authenticom does not suggest they are. Instead, this issue goes solely to damages, with Authenticom trying to trim the scope of its liability with a table of proposed cut-off dates for each counterclaim. Reynolds's damages model is calculated on a monthly basis and thus can be adapted to any ruling the Court makes. But Authenticom's asserted dates are wrong as to Reynolds's claims for the reasons set forth below.

A. Reynolds's Counterclaims Relate Back to the Original Complaint

Reynolds's counterclaims against Authenticom relate back to the date of the Original Complaint (May 1, 2017). All limitations periods should be calculated from that baseline. Authenticom asks the Court to adopt the minority view that compulsory counterclaims cannot relate back as a matter of law. Mot. 63-64. While it remains correct that the Seventh Circuit has not definitively addressed this issue, the Northern District of Illinois has adopted the well-reasoned logic of the majority position. *See Seitz v. Beeter*, 2013 WL 409428, at *2 (N.D. Ill. Jan. 31, 2013). That is consistent with dicta from the Seventh Circuit, *Asset Allocation & Mgmt. Co. v. W. Employers Ins. Co.*, 892 F.2d 566, 571 (7th Cir. 1989), and has been previously adopted by this Court, Dkt. 749 at 12-13. The Court should decline to overturn that law.

The correct test for the relation-back analysis is whether Reynolds's counterclaims arise from the same transaction or occurrence as Authenticom's claim—i.e., whether they are "logically related" to Authenticom's claim. *See Burlington N. R.R. Co. v. Strong*, 907 F.2d 707, 711 (7th Cir. 1990). "The purpose behind the rule is judicial economy; to avoid a multiplicity of actions by resolving in a single lawsuit all disputes that ensue from a common factual background." *In re Price*, 42 F.3d 1068, 1073 (7th Cir. 1994). Laying out the claims and counterclaims at issue here readily demonstrates that they are logically related—indeed, they are two competing legal visions of the same core facts. Authenticom alleges that Reynolds's efforts to prevent it from accessing the Reynolds DMS were an antitrust violation; Reynolds alleges that Authenticom's efforts to access the Reynolds DMS were a violation of multiple statutes and Reynolds's contracts. Relation-back is therefore appropriate.

To take the sharpest example, Reynolds's DMCA claim is all but pleaded on the face of Authenticom's complaint. Authenticom leads by alleging that "Reynolds started to block data integrators – including Authenticom and CDK – from accessing dealer data on the Reynolds DMS by disabling the integrator's dealer-created login credentials." Defs. JSUF Ex. 90 (Authenticom Complaint [No. 17-cv-318 (W.D. Wis.) Dkt. 1]) ¶ 6 [hereinafter *Auth.* Dkt. 1]. That "disabling" is a direct reference to Reynolds's Suspicious User ID measure, one of the primary bases for Reynolds's DMCA claim. *See also, e.g., id.* ¶ 103 ("Like CDK, Reynolds blocks third-party access to dealer data, disabling credentials created by dealers for other data integrators.").

The complaint later pleads Reynolds's specific DMCA measures in even greater detail:

> Reynolds first started disabling Authenticom's usernames in 2009 when it introduced gimmicks such as "challenge questions" and "captcha" (where the user has to enter random blurred text) to make it more difficult to automate the pulling of data. Reynolds also targeted Authenticom's usernames for specific vendors, disrupting the data flow for those vendors and thereby forcing them to join the RCI program. In June 2013, Reynolds intensified its tactics by disabling Authenticom's usernames en masse. . . . Over a three-month period in the summer of 2013, Reynolds disabled 27,000 profiles used by Authenticom at over 3,600 dealers.

Id. ¶ 189. Those very same facts form the core of Reynolds's DMCA claim. *See* Dkt. 225 ¶¶ 50-53, 70, 73-77, 124-135. The complaint also contains references to Authenticom's efforts to circumvent Reynolds's DMCA controls, attempting to spin them as antitrust injuries instead. *See, e.g., Auth.* Dkt. 1 ¶ 195 (stating that Authenticom had to devote the majority of its workforce and hire 50 temporary employees to "navigate around the shutdowns"). Indeed, Authenticom's complaint repeatedly makes clear that Reynolds's DMCA "blocking" measures caused business disruptions and were the source of Authenticom's alleged antitrust damages. *Id.* ¶¶ 14, 232. Authenticom's lead demand for injunctive relief was for the court to "enjoin[] Defendants from blocking independent data integrators"—i.e., to order Reynolds to remove the DMCA measures from its DMS. *Id.* ¶ 18. Allegations regarding Reynolds's "blocking" measures against

Authenticom are littered throughout the complaint, and context makes clear that those blocking measures are the very same technological measures that form the basis for Reynolds's DMCA claim.[51] There can be no dispute that Reynolds's DMCA claim is logically related to Authenticom's complaint.

The complaint also contains extensive allegations that support (or at a minimum, relate to) Reynolds's other counterclaims. One of Authenticom's primary antitrust theories was that Reynolds's DMS contracts with dealers contained illegal exclusive dealing provisions because they prohibit dealers from handing out usernames to third parties like Authenticom. *See, e.g., Auth.* Dkt. 1 ¶ 11. Authenticom's Second Cause of Action is founded on these contractual provisions, *id.* ¶ 255, as are multiple sections of the complaint, including both parts of section III(B)(1) ("Defendants' DMS Contracts with Dealers Grant Defendants an Exclusive Right to Access the Dealers' Data"). Those very same "exclusive dealing" provisions are the basis for Reynolds's tortious interference claim because they prohibit third-party access to the DMS. *See* Dkt. 225 ¶¶ 2, 8, 54-66, 151-56.[52] Authenticom knowingly and persistently induced dealers to violate those provisions. Authenticom also attempted to have those provisions legally invalidated as anticompetitive in its complaint. *See Auth.* Dkt. 1 ¶ 18.

Similarly, the core facts that comprise Reynolds's CFAA, WCCA, and CCCDAFA claims are pleaded in the complaint—that Authenticom accessed Reynolds's DMS, that the Reynolds DMS is a computer used in interstate commerce, that Authenticom did not have authorization from Reynolds to access the DMS, and that Authenticom obtained information from the DMS. *Auth.*

[51] *See Auth.* Dkt. 1 ¶¶ 24, 43, 74, 106, 116, 118, 119, 121, 125, 131, 148, 153, 178, 187, 190, 194, 198, 200, 209, 217, 220, 227, 233, 235, 239, 245, 273, 274, 280, 284.

[52] Authenticom's sole challenge to Reynolds's tortious interference claim is its newfangled interpretation of Reynolds's dealer licenses (Mot. 38), which fails for the reasons explained in Section I.

Dkt. 1 ¶¶ 26, 55, 78, 150. Reynolds's cease and desist letter—a kill shot to any claim that Authenticom did not know its access was unauthorized—is pleaded in detail. *Id.* ¶ 185.

Reynolds's copyright claim appears as well. From the outset, Authenticom makes clear that it provides its "integration" services by accessing the DMS using a dealer-provided username and password. *See id.* ¶ 9. That action by Authenticom is the very thing that causes an unlicensed copy of Reynolds's software to be made. Although Authenticom attempts to gloss over this, the complaint makes clear when and how the technological step of copying occurs: "Once dealers set up those credentials, the data integrator can automate the pulling of data through user emulation. The user emulation software runs the data reports and captures the data, using the database software in the same way as a user at a dealership would. The only difference is that the integrator automates the process, whereas a user at the dealership would retrieve the data manually." *Id.* ¶ 55. The previously discussed facts regarding Reynolds's DMS contracts further make clear that Authenticom's copying of the DMS software is unlicensed.

Reynolds's counterclaims also constitute one of its primary defenses against Authenticom's antitrust theories, as addressed in Defendants' Motion for Summary Judgment. *See* Dkt. 966 at 56-63. Authenticom similarly asserts that its affirmative claims constitute a defense to Reynolds's claims. *See* Dkt. 517 at 63 ("As detailed in Authenticom's complaint, Reynolds's actions and contracts purporting to prohibit Authenticom's business activities are part of an unlawful scheme to eliminate competition. As such, the contractual and legal restrictions alleged herein are void as a matter of law."). Again, Authenticom's complaint and Reynolds's counterclaims are focused on an identical core of facts, viewed through two competing legal lenses. This degree of overlap readily meets the relation-back standard. *Burlington*, 907 F.2d at 711.

B. This Court's Prior Ruling Is Not to the Contrary

This Court previously held that CDK's counterclaims against the dealers did not relate back. *See* Dkt. 749. This is distinguishable: Authenticom's original complaint was directly targeted at Reynolds's alleged acts of blocking and interference to a much greater degree than the dealers' complaint, and those very acts of "blocking" and "interference" are the nucleus of Reynolds's counterclaims. Numerous other elements central to the counterclaims—such as Authenticom's allegations regarding Reynolds's DMS contracts—were also absent in part or whole from the dealership complaint. Authenticom also tied its alleged theories of harm and requests for injunctive relief directly to Reynolds's contracts and DMCA measures, which the dealers did not. Relation-back requires the Court to consider the totality of the claims, and the totality here overlaps to an even more compelling degree than did the CDK-dealer claims.

Respectfully, the Court's prior analysis of CDK's dealer counterclaims also applied an unduly narrow version of the relation-back test: *Moore v. New York Cotton Exch.*, 270 U.S. 593, 609-10 (1926), is directly on point. But the Court need not revisit that issue to rule in Reynolds's favor. The details set forth above establish that relation-back is appropriate here.

C. At the Latest, Reynolds's Limitations Periods Run From When It First Filed Its Counterclaims in July 2017

Even if the Court disagrees with the relation-back argument, Authenticom's dates are still wrong because it ignores the fact that Reynolds originally filed its counterclaims in July 2017, not June 2018. *See Authenticom* [No. 18-868 (N.D. Ill.)] Dkt. 180. Specifically, Reynolds filed the original version of its counterclaims on July 21, 2017, shortly after the initiation of litigation. *Id.* Authenticom subsequently demanded that Reynolds withdraw that filing, asserting that Reynolds could not properly file counterclaims until after the court ruled on the pending motions to dismiss and Reynolds filed an answer. *See Auth.* Dkt. 190 (asking the court to dismiss or strike Reynolds's counterclaims as procedurally premature). Rather than disputing the procedural point, Reynolds agreed to withdraw its counterclaims and re-file them after the motions to dismiss were resolved. *See Auth.* Dkt. 200 at 2 n.3. Reynolds subsequently did just that after the case had been moved into this MDL proceeding and the motions to dismiss were resolved. *See* Dkt. 225.

Under Rule 15, Reynolds's live counterclaims relate back to July 2017. Whether or not that document was procedurally premature is irrelevant—Reynolds, at a minimum, "attempted to" set out its claims against Authenticom in that document, which is all the Rule requires. *See* Fed. R. Civ. P. 15(c)(1)(B). Reynolds's original counterclaims are substantively identical to its current ones. Reynolds added several new legal theories, but the core occurrence was the same: Authenticom's longstanding, illegal campaign to invade and take advantage of Reynolds's proprietary DMS. The purpose of relation-back is "to balance the interests of the defendant protected by the statute of limitations with the preference expressed in the Federal Rules of Civil Procedure in general, and Rule 15 in particular, for resolving disputes on their merits." *Krupski v. Costa Crociere S. p. A.*, 560 U.S. 538, 550 (2010). Authenticom had full notice of Reynolds's claims in July 2017; allowing Authenticom to escape liability for nearly 11 months of its actions merely due to a delay in the motion-to-dismiss ruling would be an extreme and unfair windfall.

IV. Reynolds Satisfies the CFAA's Jurisdictional Threshold

Because Authenticom's access was unauthorized, as set out in Section I, Authenticom's "authorization" defense to the CFAA and state analogues (Mot. 34-37) fails. Further, Reynolds revoked any purported authorization by, *inter alia*, a cease and desist letter, Resp. Auth. SOF 28, which was effective for the reasons stated in CDK's brief, *see* CDK SJ Opp. § I.C.

Authenticom's "impermissible aggregation" argument (Mot. 65-68) rests on a misinterpretation of Reynolds's CFAA claim. Reynolds would have incurred its loss—the amount it spent investigating, responding to, and protecting the DMS—regardless of the number of discrete intrusions by Authenticom. Each intrusion was an independent, concurrent cause of the whole loss. In any event, the CFAA does not prohibit aggregation of loss across intrusions by the same defendant, against the same victim, into the same computer, by the same means, in the same year. For good reason, no court—in the nearly 20 years since its enactment—has applied Authenticom's purportedly "critical parenthetical" (Mot. 68) to prohibit a civil action under the CFAA.

A. Concurrent Causation Is Not Aggregation

Reynolds has not "aggregated" losses. Reynolds has conservatively spent [redacted] per year (orders of magnitude more than $5,000) in labor costs to investigate and respond to unauthorized third-party access to its DMS, and to prevent further such access. Defs. JSOAF 71. Under the CFAA, those costs are "loss" that count toward the $5,000 jurisdictional threshold. 18 U.S.C. §§ 1030(e)(11), 1030(c)(4)(A)(i)(I); *see, e.g.*, *Svanaco, Inc. v. Brand*, 417 F. Supp. 3d 1042, 1059 (N.D. Ill. 2019) ("wasted or diverted employee time falls squarely under the CFAA's definition of loss"); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (sufficient loss where "employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to [defendant's] actions").

Reynolds's loss from investigating, responding to, and prohibiting further unauthorized third-party access was concurrently caused by each unauthorized intrusion that necessitated Reynolds's efforts. Professor Rubinfeld explained [redacted] And when multiple acts would each have caused an indivisible injury, with or without the other acts, each individual act caused the whole injury. *Watts v. Laurent*, 774 F.2d 168, 179 (7th Cir. 1985) ("It is axiomatic that where several independent actors concurrently or consecutively produce a single, indivisible injury, each actor will be held jointly and severally liable for the entire injury."). It would be "improper" to allocate portions of the indivisible injury to each concurrent cause "where either cause would have been sufficient in itself to bring about the result, as in the case of merging fires which burn a building." *United States v. NCR Corp.*, 688 F.3d 833, 839 (7th Cir. 2012) (quoting Restatement (Second) of Torts § 433A cmt. i).

Exhaustive descriptions of the costs of Reynolds's efforts are unnecessary to show that Reynolds's loss was concurrently caused by each of the unlawful intrusions, including Authenticom's. Reynolds need only show that "a reasonable jury could find that the $5,000 threshold has been exceeded." *Svanaco*, 417 F. Supp. 3d at 1059 n.9. An example suffices. [redacted]

A reasonable jury should find that Reynolds would have incurred these costs if there were any unauthorized third-party access into its system, regardless of how frequent the individual intrusions were.[53] Reynolds has waged an extensive (and costly) campaign against unauthorized third-party access "[s]ince approximately 2006." Mot. 16; RSUF 10-20; Defs. JSOF 80-88. The

[53] *See, e.g.*, *Ticketmaster L.L.C. v. Prestige Ent. West, Inc.*, 315 F. Supp. 3d 1147, 1171, 1173-74 (C.D. Cal. 2018) (plaintiff's losses flowed from "continued breach," not any particular "one-time breach," where it alleged lump-sum costs incurred to identify and defend against defendant's more than 300,000 instances of CFAA violations).

costs of that campaign are as traceable to a given instance of Authenticom's unlawful access as they are to each and every other such instance.

B. The CFAA's Jurisdictional Threshold Has No "Single Intrusion" Requirement

In any event, the CFAA does not require Reynolds to "attribute $5,000 or more in loss to any single instance of access." Mot. 68. Reynolds alleges that Authenticom violated Section 1030(a)(2)(C) of the CFAA because it "obtain[ed] . . . information from a[] protected computer" by "intentionally access[ing] a computer without authorization." 18 U.S.C. § 1030(a)(2)(C); Dkt. 225 at ¶ 103. The "protected computer" is the Reynolds DMS. *Id.* ¶ 104.[54]

Section 1030(g) provides a right of action for any person "who suffers damage or loss by reason of" a CFAA violation. The breadth of Section 1030(g) creates the reason for the $5,000 jurisdictional threshold. The problem is that, left only to its first sentence, Section 1030(g) would create a federal crime out of, say, "a teenage hacker . . . play[ing] a trick on a friend by modifying the friend's vanity Web page." Statement of Sen. Leahy (Oct. 24, 2000), 146 Cong. Rec. S10913, S10915, 2000 WL 1585992. Hence the $5,000 threshold, which serves to moderate a statute that would otherwise "have over-federalized minor computer abuses." *Id.*

Despite Authenticom's protestations, Congress did not intend to treat cases like this one, in which thousands of unauthorized intrusions cause millions in losses, as minor. Under Section 1030(g), the jurisdictional thresholds are met so long as the defendant's "conduct involves 1 of the factors set forth." By speaking in terms of what the defendant's conduct must "involve" (rather than what each distinct violation must entail), this provision belies the notion that every single intrusion must individually meet a jurisdictional threshold. But even if Authenticom were correct

[54] Authenticom's Motion does not suggest that the Reynolds DMS is not a "computer" within the CFAA's definition, which includes "any data storage facility or communications facility directly related to or operating in conjunction with" a computer. 18 U.S.C. § 1030(e)(1).

that the "term 'the conduct' refers to the underlying (singular) violation'" (Mot. 66), that would not prohibit aggregation, either. This Circuit recognizes that, lest two $4,000 violations be treated as somehow less worthy of federal intervention than one $5,000 violation, aggregation must be permitted across acts that would individually not meet a minimum-loss threshold—even when the threshold is an element of the violation. *See, e.g.*, *United States v. Yashar*, 166 F.3d 873, 876 (7th Cir. 1999) (regarding offense of conversion of federal property "valued at $5,000 or more," if a defendant "stole $500 per month for 10 months," the "amounts can be aggregated to meet the $5,000 statutory minimum").

Neither does Authenticom's so-called "critical parenthetical" (Mot. 68), inserted into the CFAA in 2001, require that the loss to a private plaintiff have resulted from a single intrusion. The parenthetical says nothing about what is required of private plaintiffs. And the remainder of the provision explicitly contemplates that their loss may be "aggregat[ed]" over a "1-year period":

> loss to **1 or more** persons during any **1-year period** (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) **aggregating** at least $5,000 in value.

18 U.S.C. § 1030(c)(4)(A)(I). Tellingly, Authenticom cites no case in which a court has read the parenthetical to undermine the language of aggregation outside the parenthetical. Even putting aside the direct reference to "aggregating," it would be nonsensical to premise liability on losses sustained over a yearlong period if Congress's focus were only on single intrusions. As explained in the only circuit-level authority on the subject, the "syntax makes it clear that . . . the $5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a

particular intrusion." *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004). District courts agree.[55]

Authenticom is wrong to suggest that its reading alone "give[s] meaning to the parenthetical." Mot. 66. Authenticom would have the Court read the parenthetical to expand the government's scope of aggregation to include loss from any "related course of conduct" (and thus by negative implication deny such aggregation to private plaintiffs). But Authenticom misreads the parenthetical. It grants the government the ability to aggregate across multiple *computers*, and the "related course of conduct" phrase *limits* that grant. It speaks to the degree to which CFAA violations affecting multiple computers must be similar (or otherwise related) for the government to aggregate losses from each affected computer. The parenthetical clearly requires that if the government aggregates losses across multiple computers, the conduct causing those losses must be related. But it says nothing about aggregation across intrusions into a single computer system.[56]

[55] *See Wolf v. Schadegg*, 2016 WL 1117364, at *3 (D. Colo. Mar. 21, 2016) ("[M]any other courts have rejected Defendants' argument that $5,000 threshold be met with respect to each particular intrusion."); *Freedom Banc Mortg. Services, Inc. v. O'Harra*, 2012 WL 3862209, at *6-7 (S.D. Ohio Sept. 5, 2012) (rejecting argument that "Plaintiff fails to identify an unauthorized intrusion that, itself, caused a $5,000 loss" as having been "persuasively rejected"); *Sprint Nextel Corp. v. Simple Cell, Inc.*, 2013 WL 3776933, at *7 (D. Md. July 17, 2013) ("[Plaintiff] must only have alleged that, taken together, a defendant's violations over a 1-year period caused enough loss or damages.").

Authenticom's contrary authority predates the supposedly "critical" (Mot. 68) parenthetical. *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). Indeed, it is doubly outdated, having relied for its textual theory on a provision no longer applicable to Reynolds's claim. As this Court recognized, *DoubleClick*'s textual theory was that the CFAA required damages or losses totaling $5,000 to have been caused by an "impairment," which the court took to require a "single act" because "impairment" was "phrased in the singular." 154 F. Supp. 2d at 523; *see In re DMS Antitrust Litig.*, 2019 WL 4166864, at *12 (N.D. Ill. Sept. 3, 2019). That was wrong even then, because "[m]ultiple intrusions can cause a single impairment." *Creative Computing*, 386 F.3d at 934. But regardless, CFAA claims like Reynolds's now run through the CFAA's definition of "loss," which unlike the definition of "damage" makes no reference to the singular term "impairment" and is instead broadly defined to include "any reasonable cost to any victim," *id.* § 1030(e)(11); *see also In re DMS*, 2019 WL 4166864, at *11 n.7 ("Section 1030(c)(4)(A)(i)(I) does not address damage."). This change, like the addition of the "critical" parenthetical, resulted from the 2001 amendments. *See* Pub. L. No. 107-56, § 814, 115 Stat. 272 (Oct. 26, 2001).

[56] For this reason, Authenticom misplaces its reliance on dictum in *Mount v. Pulse Point, Inc.*, 2016 WL 5080131, at *9 n.4 (S.D.N.Y. Aug. 17, 2016), and certain history similarly discussing aggregation across multiple computers. Mot. 67.

If any doubt remains, Authenticom's reading fails because "statutes have to be interpreted to avoid absurd results." *Senne v. Village of Palatine, Ill,,* 784 F.3d 444, 447 (7th Cir. 2015). According to Authenticom, if Reynolds spent $5,000 responding to a single instance of unauthorized access, Reynolds has a CFAA claim; but if Reynolds spent the very same $5,000 responding to two instances of unauthorized access, Reynolds has no CFAA claim. Recurrent unauthorized access cannot be absolved by its recurrence. *See Creative Computing*, 386 F.3d at 935 (rejecting the same "single intrusion" argument because that "construction would attribute obvious futility to Congress rather than rationality, because a hacker could evade the statute by setting up thousands of $4,999 (or millions of $4.99) intrusions"); *see also United States v. Webb*, 691 F. Supp. 1164, 1168 (N.D. Ill. 1988) (explaining that it is because "aggregation is permissible" across multiple conversions of federal property that clever criminals cannot "escape the federal government's power" by "mak[ing] sure each theft is under $5,000").

V. Authenticom Does Not Take Issue with Reynolds's UCL Claim for Injunctive Relief

Authenticom challenges Reynolds's claim for damages under the California UCL. Mot. 71-72. To narrow the issues, Reynolds withdraws any claim for damages under the California UCL. Authenticom does not, however, challenge Reynolds's claim for an injunction under the California UCL. Dkt. 225 ¶ 179; *see also Kwikset Corp. v. Superior Court*, 246 P.3d 877, 895 (Cal. 2011) ("Injunctions are the primary form of relief available under the UCL . . . .").

VI. Ample Evidence of Injury Supports Reynolds's Trespass to Chattel Claim

Authenticom's unauthorized access to Reynolds's DMS (1) "impaired" the DMS "as to its condition, quality or value"; (2) "deprived" Reynolds of the exclusive "use of the [DMS] for a substantial time"; and (3) otherwise caused harm to "thing[s] in which [Reynolds] has a legally protected interest." *Wis. Tel. Co. v. Reynolds*, 87 N.W.2d 285, 288 (Wis. 1958); *see also* Restatement (Second) of Torts § 218. Each injury independently supports Authenticom's liability in trespass to chattel. And contrary to Authenticom's suggestion (Mot. 38-39), Reynolds's trespass to chattel claim is viable regardless of whether Authenticom was an authorized "agent" under Reynolds's dealer licenses. As set out in CDK's brief, the common law of trespass contemplates revocation of consent, CDK SJ Opp. § I.C, and Reynolds clearly revoked any consent by, *inter alia*, a cease and desist letter in early 2015. Resp. Auth. SOF 28. Moreover, Reynolds's licenses independently prohibited the *means* of Authenticom's access. *Supra* Section I.B.2. Authenticom therefore "exceed[ed]" any purported consent, which consent "is not effective for the excess." Restatement (Second) of Torts § 892A(4); *see also Grygiel v. Monches Fish & Game Club, Inc.*, 787 N.W.2d 6, 18 (Wis. 2010) ("[W]hen an easement holder's use of an express easement contravenes its express terms, . . . the easement holder may be held liable for trespass.").

The injury to Reynolds's possessory interest in its DMS is alone sufficient to support its trespass to chattel claim given the frequency of Authenticom's unauthorized access. Because Authenticom's trespasses used up computing capacity that would otherwise be usable by Reynolds, Authenticom deprived Reynolds of that capacity. *See Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 250 (S.D.N.Y. 2000). Even occupying a small amount of that capacity is sufficient. *See eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000). Authenticom ran unauthorized queries on the Reynolds DMS [redacted], which is plenty for a jury to conclude that this deprivation was "for a substantial time." [redacted]; *Reynolds*, 87 N.W.2d at 288. To be sure, Authenticom notes a few courts that have held that unauthorized access does not alone suffice. Mot. 74. But those cases are a far cry from this one: Authenticom has run [redacted] on the Reynolds

DMS. Defs. JSOAF 73; *compare Intel Corp. v. Hamidi*, 71 P.3d 296, 299 (Cal. 2003) (claim based on six emails over two years).[57]

Regardless, there is evidence supporting an inference of actual injury beyond deprivation of Reynolds's interest in exclusive possession. Authenticom's trespasses increased the burden on Reynolds's DMS and thereby affected its performance. *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004) (trespass to chattel claim supported where defendant's software robots "perform[ed] multiple automated successive queries" and "consumed a significant portion of the capacity of [plaintiff's] computer systems," though they "alone would not incapacitate [plaintiff's] systems"); *Sotelo v. DirectRevenue, LLC*, 384 F. Supp. 2d 1219, 1231 (N.D. Ill. 2005) (trespass to chattel claim supported by evidence of "over-burdening" and "diminishing . . . functioning"). [redacted]

[57] *Compare also Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000) (number of "hits" traced to defendant was "very small" compared to other users); *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 412 (S.D.N.Y. 2018) (single employee copied files onto a personal hard drive).

[redacted][58]

Authenticom's trespasses also harmed Reynolds's customer goodwill—that is, "a thing in which [Reynolds] has a legally protected interest." *Reynolds*, 87 N.W.2d at 288; *Chuck Wagon Catering, Inc. v. Raduege*, 277 N.W.2d 787, 792 (Wis. 1979) ("customer goodwill has been recognized as a property interest in and of itself"). [redacted] That harm to customer goodwill supports liability in trespass to chattel. *See CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) ("Defendants' intrusions into CompuServe's computer systems, insofar as they harmed plaintiff's business reputation and goodwill with its customers, are actionable under Restatement § 218(d).").

VII. Reynolds's Contracts With *Dealers* Do Not Undermine Its Unjust Enrichment Claim Against *Authenticom*

Briefly, Authenticom's passing attempt to fit this case into those in which a benefit was "voluntarily conferred" (Mot. 40) is meritless—Reynolds made abundantly clear that Authenticom's access to the Reynolds DMS was anything but voluntarily given, including by way of a cease and desist in early 2015. Resp. Auth. SOF 28.

[58] Authenticom makes much of Reynolds's not definitively tracing certain instances of performance problems to Authenticom alone. Mot. 73. [redacted]

Authenticom contests neither the fact that it benefitted from access to Reynolds's DMS nor the fact that it has paid nothing for that benefit. Instead, it relies on Reynolds's contracts with dealers, suggesting that "[w]ell-settled law precludes an unjust enrichment claim for a subject governed by a contract, even where that contract is with a third party." Mot. 7. That is not the law (much less "well-settled" law).

There is good reason to reject unjust enrichment claims when a proper contract exists *between the plaintiff and the defendant*. To "prevent injustice," equity implies a "quasi contract" between the beneficiary and the benefitter. *Watts v. Watts*, 405 N.W.2d 303, 313 (Wis. 1987). So courts naturally prohibit unjust enrichment claims between parties that have an actual contract because there is nothing to imply and there is no injustice. *See Shimko v. Jeff Wagner Trucking, LLC*, 2013 WL 10075919, at *5 (W.D. Wis. June 28, 2013). But that rule has no application to Authenticom, which obtained a benefit for which it never bargained. *See Griswold v. Antoniak*, 828 N.W.2d 594, at *4 (Wis. Ct. App. 2013) (rejecting application of this rule when the defendant is "*not* . . . a party, or in privity with a party, to the contract"); *see also RehabCare Grp. East, Inc. v. SAK Mgmt. Servs., LLC*, 2010 WL 3307084, at *3 (N.D. Ill. Aug. 18, 2010) (finding "no support in the case law to suggest" that the rule barring unjust enrichment in the presence of a contract applies to "those who are not parties to the contract").[59]

Authenticom's purportedly "on point" case is anything but on point. Mot. 75. It is a construction case where a general contractor failed to pay a subcontractor, and the subcontractor sued the owner for unjust enrichment. *Gebhardt Bros., Inc. v. Brimmel*, 143 N.W.2d 479, 481-82 (Wis. 1966). But the Wisconsin Supreme Court has made explicitly clear that the reason the subcontractor had no claim for unjust enrichment against the owner was not the mere existence of

[59] *RehabCare* applies Illinois unjust enrichment law, which is "similar to that of Wisconsin." *Beer Capitol Distrib., Inc. v. Guinness Bass Import Co.*, 290 F.3d 877, 881 (7th Cir. 2002).

a contract between the owner and the general contractor. The "critical factor" in *Gebhardt* and similar "cases involving subcontractors" was "that the defendant *had paid another for the benefits conferred*, and thus it was not inequitable to permit the defendant to retain the benefits without paying the plaintiff." *S & M Rotogravure Serv., Inc. v. Baer*, 252 N.W.2d 913, 918 (Wis. 1977) (emphasis added); *see also Gebhardt*, 143 N.W.2d at 481 ("the evidence indicates that the owner has either paid the general contractor for the benefits furnished or is obligated to do so"). When "[t]here is no suggestion that the defendant has paid for the benefits," the subcontractor cases are "inapposite." *Puttkammer v. Minth*, 266 N.W.2d 361, 364 (Wis. 1978).[60] And it is undisputed that Authenticom has paid neither Reynolds nor dealers for the benefit of access to Reynolds's DMS.

Not only that, but Reynolds's contracts with dealers do not set the price or other terms of Authenticom's access to the DMS. To the contrary, they prohibit that access. *Supra* Section I. Subcontractor cases exist in a different realm, where the plaintiff and defendant share the same bargain via a third-party intermediary. In contrast, Reynolds's contracts with dealers say nothing about Authenticom's bargain for DMS access, because there is no such bargain. They thus do not "cover[] the aspect relevant to [Reynolds's] unjust enrichment claim" and could not bar it even if Authenticom were a party to them. *N. Crossarm Co., Inc. v. Chem. Specialties, Inc.*, 318 F. Supp. 2d 752, 766 (W.D. Wis. 2004); *see also Liberty Mut. Ins. Co. v. Lund*, 2020 WL 2514120, at *1 (W.D. Wis. May 15, 2020) ("Wisconsin law does not bar a party from seeking equitable relief for a benefit conferred, if that benefit falls outside the scope of the parties' contractual relationship.").

[60] Authenticom's only other cited authority also involves a subcontracting situation. The plaintiff purchased items from one defendant, who subcontracted the order to the other defendant. Both contracts were performed. *See Emirat AG v. High Point Printing LLC*, 248 F. Supp. 3d 911, 924 (E.D. Wis. 2017) ("Emirat paid High Point a total sum of over $700,000 for the printing of the scratch-off cards at issue in this case. WS Packaging was paid a lesser sum by High Point for this project."). So again, there is no analogy to this case.

VIII. Authenticom Is Liable for Fraud Because It Knowingly Misrepresented Its Access as Authorized and Human

Authenticom falsely represented that it was an authorized user (as opposed to an unauthorized third party) each time it accessed Reynolds's DMS. And it falsely represented that it was accessing the Reynolds DMS by human means (as opposed to automated means) each time it answered one of Reynolds's CAPTCHA prompts. Authenticom's argument to the contrary (Mot. 77-78) rests on an overly narrow conception of what constitutes a "misrepresentation." Wisconsin law "liberally construe[s] certain conduct as a misrepresentation." *Bay State Milling Co. v. Martin*, 916 F.2d 1221, 1228 (7th Cir. 1990); *see also John Doe 1 v. Archdiocese of Milwaukee*, 734 N.W.2d 827, 840-41 (Wis. 2007). Indeed, "[a]ny conduct capable of being turned into a statement of fact is a representation." *Lundin v. Shimanski*, 368 N.W.2d 676, 681 & n.5 (Wis. 1985) (explaining why defendant's "act of accepting [an] offer" could constitute fraud); *see also Estate of DeWitt v. DeWitt*, 333 N.W.2d 733, at *6 (Wis. Ct. App. 1983) (finding sufficient evidence of misrepresentation from the "impression [defendant] created").

When Authenticom entered a username and password on the Reynolds DMS, it falsely conveyed that it was a licensed user and not an unauthorized third party. Reynolds's login screens explicitly state that "*This software may not be* copied, disclosed, decompiled, disassembled, shared with or *accessed by a third party* electronically or manually." Mot. 78. A jury could reasonably find that by entering access credentials in the face of an explicit statement that third-party access is unauthorized, Authenticom misrepresented itself as something other than an unauthorized third party. *See 1st Team Tech., Inc. v. Sys. Eng'g, Inc.*, 2012 WL 12873551, at *2 (N.D. Fla. June 12, 2012) (recognizing fraud claim where unauthorized third party accessed plaintiff's "password protected website" using a password from plaintiff's authorized client).

Similarly, when Authenticom used automated means to circumvent Reynolds's CAPTCHA prompts, it falsely conveyed that a human was inputting the information, and that a human would use Reynolds's DMS after answering the prompt. The exemplar Reynolds CAPTCHA cited in Authenticom's motion literally states that "human interaction is required." Mot. 51. [redacted] Authenticom thus misrepresented itself as a human user and falsely confirmed its compliance with the CAPTCHA prompt's requirement. *See United States v. Lowson*, 2010 WL 9552416, at *2 (D.N.J. Oct. 12, 2010) (recognizing criminal fraud charge where defendants used "automated software to defeat the vendors' security measures, including CAPTCHA," used "CAPTCHA Bots to quickly solve CAPTCHA challenges," and "created a database of CAPTCHA challenges and their answers," among other things).[61]

Alternatively, Authenticom achieved unauthorized, automated access to the Reynolds DMS through material omissions that are equally actionable in fraud. When it sought to access Reynolds's DMS, Authenticom had—and violated—a duty to disclose that it was an unauthorized third party accessing the system by automated means. A reasonable jury would understand Authenticom's answers to Reynolds's login and CAPTCHA prompts as "half-truth[s]," technically satisfactory to bypass the prompts but "creat[ing] a false impression" about who was accessing the system (a licensed dealer employee, not an unlicensed third party) and in what manner (human, not automated, means). *See Ollerman v. O'Rourke Co., Inc.*, 288 N.W.2d 95, 102 (Wis. 1980). They thus created a duty to disclose the full truth. *Id.* at 30-31. Further, as conclusively

[61] Like civil fraud in Wisconsin, wire fraud, which was charged in *Lowson*, requires a misrepresentation or omission. *Livingston v. Shore Slurry Seal, Inc.*, 98 F. Supp. 2d 594, 597 (D.N.J. 2000).

demonstrated by Reynolds's longstanding and well-publicized prohibition on unauthorized, automated access (*see* RSUF 10-19; Defs. JSUF 80-88), these undisclosed facts were "material" to Authenticom's achieving entry; Authenticom knew that it only obtained access due to Reynolds's "mistake" as to these facts; and Reynolds should have been known to "expect" disclosure of the fact that, contrary to Reynolds's well-known policy, Authenticom was an unlicensed, non-human user. *Kaloti Enters., Inc. v. Kellogg Sales Co.*, 699 N.W.2d 205, 213 (Wis. 2005). But Authenticom hid the facts, keeping them "peculiarly and exclusively within [its] knowledge," notwithstanding Reynolds's diligent efforts (*see generally supra* Section II.B), and thus violated its duty to disclose. *See Kaloti*, 699 N.W.2d at 213.

Briefly, Authenticom's suggestion that its "authorization" arguments also go to Reynolds's fraud claim is misguided, too. Mot. 40-41. Even if a jury found that Authenticom were "authorized" under Reynolds's DMS licenses, Authenticom nevertheless—by misrepresentation or omission—fraudulently held itself out as something other than a third party accessing the DMS by non-human means. So a jury could find fraud regardless of Authenticom's contractual status.

IX. There Is Evidence of Damages

Authenticom's challenge to Reynolds's damages proof should be rejected because Professor Rubinfeld's damages opinions are admissible. *See* Dkt. 994. In any event, expert testimony is not required when "the issue of damages [is] not beyond a lay juror's understanding." *Wis. Alumni Research Found. v. Xenon Pharms., Inc.*, 591 F.3d 876, 887 (7th Cir. 2010). Professor Rubinfeld's opinions are the best evidence of damages, but Authenticom is wrong to suggest they are "the only possibly competent evidence" of damages. Mot. 78-79. For example, absent Professor Rubinfeld's opinions, Reynolds of course remains entitled to statutory damages under the DMCA for each instance of unlawful circumvention by Authenticom, 17 U.S.C. § 1203(c)(3), and [redacted].

[redacted]. Reynolds could also quantify recovery in unjust enrichment through [redacted] Further, Reynolds could prove compensatory damages with its own records of labor hours and salaries, as discussed above in Section IV.A.

CONCLUSION

For the reasons stated, Authenticom's Motion for Summary Judgment should be denied.

DATE: July 28, 2020

Respectfully submitted,

/s/ *Aundrea K. Gulley*
Aundrea K. Gulley
Brian T. Ross
Brice A. Wilkinson
Ross M. MacDonald
Justin D. Patrick
Michael R. Davis
GIBBS & BRUNS LLP
1100 Louisiana Street
Suite 5300
Houston, TX 77002
(713) 751-5258
agulley@gibbsbruns.com
bross@gibbsbruns.com
bwilkinson@gibbsbruns.com
rmacdonald@gibbsbruns.com
jpatrick@gibbsbruns.com
mdavis@gibbsbruns.com

Leo D. Caseria
SHEPPARD MULLIN RICHTER & HAMPTON, LLP
2099 Pennsylvania Avenue NW, Suite 100
Washington, DC 20006
(202) 747-1900
lcaseria@sheppardmullin.com

Counsel for Defendant The Reynolds and Reynolds Company

CERTIFICATE OF SERVICE

I, Justin D. Patrick, an attorney, hereby certify that on July 28, 2020, I caused a true and correct copy of the public, redacted version of the foregoing **COUNTERPLAINTIFF THE REYNOLDS AND REYNOLDS COMPANY'S OPPOSITION TO COUNTERDEFENDANT AUTHENTICOM, INC.'S MOTION FOR SUMMARY JUDGMENT** to be served electronically on all counsel of record by operation of the CM/ECF system, and a true and correct copy of the sealed, unredacted version of same to be served electronically on all counsel of record at the following email address:

SERVICE-EXTERNAL-DMS-MDL@lists.kellogghansen.com

/s/ *Justin D. Patrick*
Justin D. Patrick